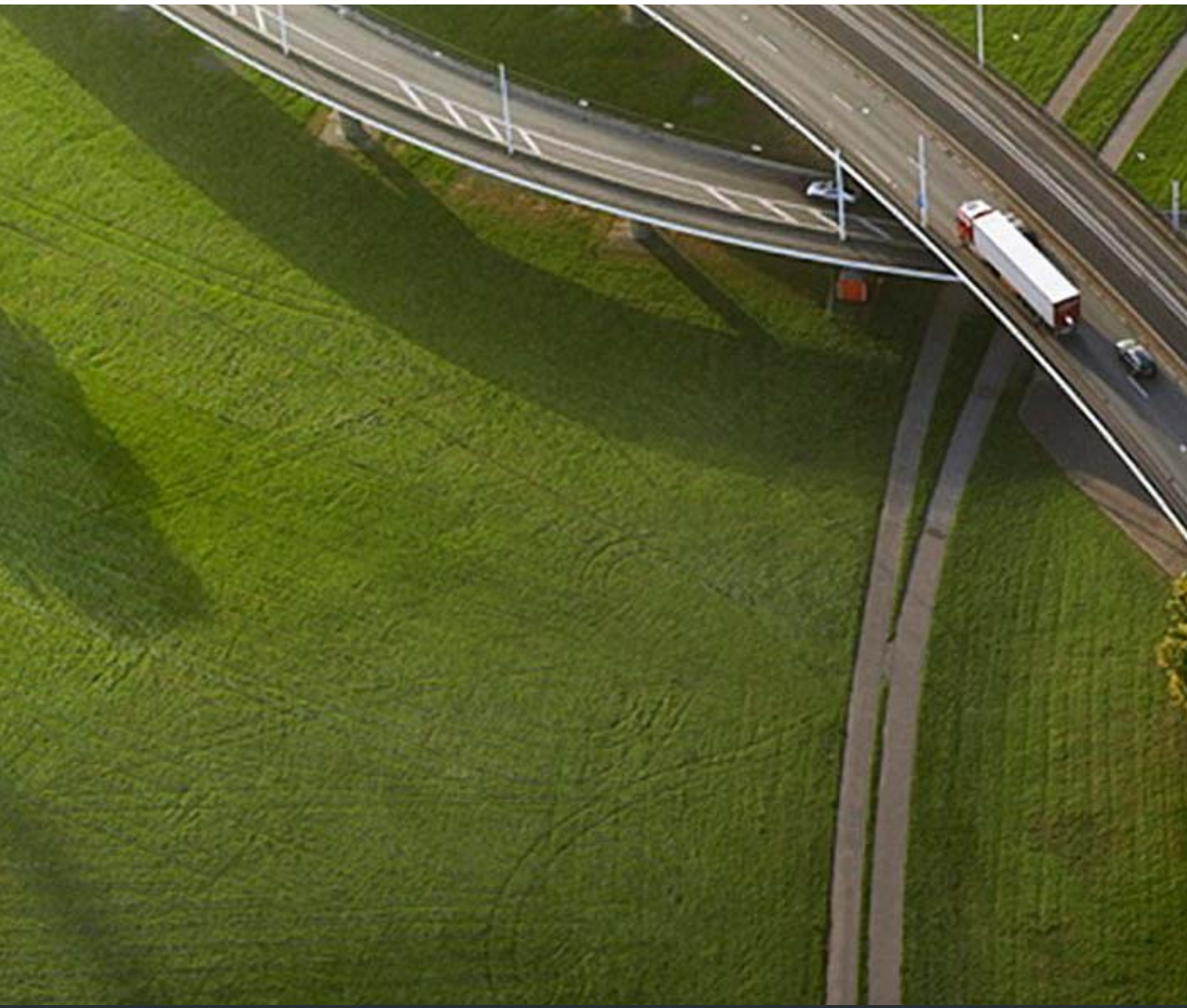
UNIFY Harmonize your enterprise



# Phone Administration
# OpenStage SIP V3R3 for OpenScape Voice

**Administration Manual**

A31003-S2030-M100-10-76A9

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Unify GmbH & Co. KG 01/2014
Hofmannstr. 51, 81379 Munich/Germany

All rights reserved.

Reference No.: A31003-S2030-M100-10-76A9

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.
An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify GmbH & Co. KG.
All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

unify Harmonize your enterprise

**unify.com**

**1 Overview . . . . . 11**
1.1 Important Notes . . . . . 11
1.2 Maintenance Notes . . . . . 12
1.3 About the Manual . . . . . 12
1.4 Conventions for this Document . . . . . 12
1.5 The OpenStage Family . . . . . 14
1.5.1 OpenStage 60/80 . . . . . 14
1.5.2 OpenStage 40 . . . . . 15
1.5.3 OpenStage 40 US . . . . . 16
1.5.4 OpenStage 20 . . . . . 18
1.5.5 OpenStage 15 . . . . . 19
1.6 Administration Interfaces . . . . . 20
1.6.1 Web-based Management (WBM) . . . . . 20
1.6.2 DLS (Deployment Service) . . . . . 20
1.6.3 Local Phone Menu . . . . . 20

**2 Startup . . . . . 21**
2.1 Prerequisites . . . . . 21
2.2 Assembling and Installing the Phone . . . . . 22
2.2.1 Shipment . . . . . 22
2.2.2 Connectors at the bottom side . . . . . 22
2.2.3 Assembly . . . . . 23
2.2.4 Connecting the Phone . . . . . 24
2.3 Quick Start . . . . . 26
2.3.1 Accessing the Web Interface (WBM) . . . . . 26
2.3.2 Set the Terminal Number . . . . . 27
2.3.3 Basic Network Configuration . . . . . 27
2.3.4 DHCP Resilience . . . . . 28
2.3.5 Date and Time / SNTP . . . . . 28
2.3.6 SIP Server Address . . . . . 29
2.3.7 Extended Network Configuration . . . . . 29
2.3.8 Vendor Specific: VLAN Discovery And DLS Address . . . . . 29
2.3.8.1 Using a Vendor Class . . . . . 30
2.3.8.2 Using Option #43 "Vendor Specific" . . . . . 38
2.3.9 Registering at Phone Administration . . . . . 43
2.4 Startup Procedure . . . . . 44
2.5 Cloud Deployment . . . . . 45
2.5.1 Process of Cloud Deployment . . . . . 45
2.5.2 Aborting cloud deployment process by User . . . . . 48
2.5.3 Re-trigger cloud deployment . . . . . 48
2.5.4 Deployment errors . . . . . 49

**3 Administration . . . . . 50**
3.1 Access via Local Phone . . . . . 50
3.2 LAN Settings . . . . . 54

3.2.1 LAN Port Settings . . . 54
3.2.2 VLAN . . . 56
3.2.2.1 Automatic VLAN discovery using LLDP-MED . . . 57
3.2.2.2 Automatic VLAN discovery using DHCP . . . 58
3.2.2.3 Manual configuration of a VLAN ID . . . 59
3.2.3 LLDP-MED Operation . . . 60
3.3 IP Network Parameters . . . 61
3.3.1 Quality of Service (QoS) . . . 61
3.3.1.1 Layer 2 / 802.1p . . . 61
3.3.1.2 Layer 3 / Diffserv . . . 62
3.3.2 Protocol Mode IPv4/IPv6 . . . 65
3.3.3 Use DHCP . . . 66
3.3.4 IP Address - Manual Configuration . . . 69
3.3.4.1 Configuration . . . 69
3.3.5 Default Route/Gateway . . . 71
3.3.6 Specific IP Routing . . . 73
3.3.7 DNS . . . 75
3.3.7.1 DNS Domain Name . . . 75
3.3.7.2 DNS Servers . . . 76
3.3.7.3 Terminal Hostname . . . 77
3.3.8 Configuration & Update Service (DLS) . . . 78
3.3.9 SNMP . . . 80
3.4 Security . . . 83
3.4.1 Speech Encryption . . . 83
3.4.1.1 General Configuration . . . 83
3.4.1.2 MIKEY Configuration . . . 84
3.4.1.3 SDES Configuration . . . 86
3.4.2 Access Control . . . 87
3.4.3 Security Log . . . 88
3.4.4 Security-Related Faults . . . 89
3.4.5 Password Policy . . . 90
3.4.5.1 General Policy . . . 90
3.4.5.2 Admin Policy . . . 91
3.4.5.3 User Policy . . . 92
3.4.5.4 Character Set . . . 92
3.4.5.5 Change Admin and User password . . . 93
3.4.6 Certificate Policy . . . 94
3.4.6.1 Online Certificate Check . . . 94
3.4.6.2 Server Authentication Policy . . . 95
3.5 System Settings . . . 96
3.5.1 Terminal and User Identity . . . 96
3.5.1.1 Terminal Identity . . . 96
3.5.1.2 Display Identity . . . 96
3.5.2 Emergency and Voice Mail . . . 98

3.5.3 Energy Saving (OpenStage 40/60/80) . . . . . 99
3.5.4 Call logging . . . . . 100
3.5.4.1 Logging of Missed Calls (via User menu) . . . . . 101
3.5.5 Date and Time . . . . . 103
3.5.5.1 SNTP is Available, but no Automatic Configuration by DHCP server . . . . . 103
3.5.5.2 No SNTP Server Available . . . . . 105
3.5.6 SIP Addresses and Ports . . . . . 106
3.5.6.1 SIP Addresses . . . . . 106
3.5.6.2 SIP Ports . . . . . 108
3.5.7 SIP Registration . . . . . 109
3.5.8 SIP Communication . . . . . 111
3.5.8.1 Outbound Proxy . . . . . 111
3.5.8.2 SIP Transport Protocol . . . . . 112
3.5.8.3 Media/SDP . . . . . 113
3.5.9 SIP Session Timer . . . . . 114
3.5.10 Resilience and Survivability . . . . . 116
3.5.10.1 TLS Connectivity Check . . . . . 117
3.5.10.2 Response Timer . . . . . 118
3.5.10.3 Non-INVITE Transaction Timer . . . . . 119
3.5.10.4 Maximum Registration Backoff Timer . . . . . 120
3.5.10.5 Backup SIP Server . . . . . 121
3.6 Feature Access . . . . . 124
3.7 Feature Configuration . . . . . 127
3.7.1 Allow Refuse . . . . . 127
3.7.2 Hot/Warm Phone . . . . . 129
3.7.3 Initial Digit Timer . . . . . 131
3.7.4 Group Pickup . . . . . 132
3.7.4.1 Feature Code . . . . . 132
3.7.4.2 Pickup alert . . . . . 132
3.7.5 Call Transfer . . . . . 135
3.7.5.1 Transfer on Ring . . . . . 135
3.7.5.2 Transfer on Hangup . . . . . 135
3.7.6 Callback URIs . . . . . 137
3.7.6.1 Call Completion . . . . . 138
3.7.7 Message Waiting Address . . . . . 139
3.7.8 Indicate Messages . . . . . 140
3.7.9 System Based Conference . . . . . 142
3.7.10 Server Based Features . . . . . 143
3.7.11 uaCSTA Interface . . . . . 145
3.7.12 Local Menu Timeout . . . . . 147
3.7.13 Call Recording . . . . . 148
3.8 Free Programmable Keys . . . . . 150
3.8.1 Clear (no feature assigned) . . . . . 151
3.8.2 Selected Dialing . . . . . 151

3.8.3 Repeat Dialing . . . 152
3.8.4 Call Forwarding (Standard) . . . 152
3.8.5 Call Forwarding by Call Type . . . 153
3.8.6 Ringer Off . . . 155
3.8.7 Hold . . . 155
3.8.8 Alternate . . . 155
3.8.9 Blind Call Transfer / Move Blind . . . 156
3.8.10 Transfer Call . . . 156
3.8.11 Deflect a Call . . . 157
3.8.12 Shift Level . . . 157
3.8.13 Phone-Based Conference . . . 157
3.8.14 Accept Call via Headset (OpenStage 40/60/80) . . . 158
3.8.15 Do Not Disturb . . . 158
3.8.16 Group Pickup . . . 159
3.8.17 Repertory Dial . . . 159
3.8.18 Hunt Group: Send Busy Status . . . 160
3.8.19 Mobile User Logon . . . 160
3.8.20 Directed Pickup . . . 161
3.8.21 Callback . . . 161
3.8.22 Cancel Callbacks . . . 162
3.8.23 Consultation . . . 162
3.8.24 Call Waiting . . . 162
3.8.25 Call recording . . . 163
3.8.26 Auto Answer With Zip Tone . . . 164
3.8.27 Server Feature . . . 164
3.8.28 BLF Key . . . 164
3.8.29 Start Application . . . 165
3.8.30 Send Request via HTTP/HTTPS . . . 165
3.8.31 Built-in Forwarding . . . 168
3.8.32 2nd Alert . . . 168
3.8.33 Start Phonebook (OpenStage 40/15 only) . . . 168
3.8.34 Show phone screen (OpenStage 15 and OpenStage 40 only) . . . 169
3.8.35 Mute (OpenStage 15 only) . . . 169
3.8.36 Release (OpenStage 15 only) . . . 169
3.9 Preset Function Keys (OpenStage 40 US only) . . . 170
3.10 Fixed Function Keys . . . 170
3.10.1 Fixed Function Keys on OpenStage 40 US . . . 170
3.11 Multiline Appearance/Keyset . . . 171
3.11.1 Line key configuration . . . 171
3.11.2 Configure Keyset Operation . . . 177
3.11.3 Line Preview . . . 183
3.11.3.1 Preview and Preselection . . . 184
3.11.4 Immediate Ring . . . 185
3.11.5 Direct Station Select (DSS) . . . 185

3.11.5.1 General DSS Settings . . . . . 186
3.11.5.2 Settings for a DSS key . . . . . 187
3.11.6 Distinctive Ringers per Keyset Lines . . . . . 189
3.12 Key Modules . . . . . 192
3.13 Dialing . . . . . 194
3.13.1 Canonical Dialing Configuration . . . . . 194
3.13.2 Canonical Dial Lookup . . . . . 198
3.13.3 Phone location . . . . . 200
3.13.4 Dial Plan . . . . . 201
3.14 Ringer Setting . . . . . 204
3.14.1 Distinctive . . . . . 204
3.14.2 Map to Specials . . . . . 206
3.14.3 Special Ringers . . . . . 207
3.15 Mobility . . . . . 210
3.16 Transferring Phone Software, Application, and Media Files . . . . . 212
3.16.1 FTP/HTTPS Server . . . . . 212
3.16.2 Common FTP/HTTPS Settings . . . . . 212
3.16.3 Phone Software . . . . . 214
3.16.3.1 FTP/HTTPS Access Data . . . . . 214
3.16.3.2 Download/Update Phone Software . . . . . 217
3.16.4 Music on Hold . . . . . 218
3.16.4.1 FTP/HTTPS Access Data . . . . . 218
3.16.4.2 Download Music on Hold . . . . . 220
3.16.5 Picture Clips . . . . . 221
3.16.5.1 FTP/HTTPS Access Data . . . . . 221
3.16.5.2 Download Picture Clip . . . . . 223
3.16.6 LDAP Template . . . . . 224
3.16.6.1 FTP/HTTPS Access Data . . . . . 224
3.16.6.2 Download LDAP Template . . . . . 226
3.16.7 Logo . . . . . 227
3.16.7.1 FTP/HTTPS Access Data . . . . . 227
3.16.7.2 Download Logo . . . . . 229
3.16.8 Screensaver . . . . . 230
3.16.8.1 FTP/HTTPS Access Data . . . . . 230
3.16.8.2 Download Screensaver . . . . . 232
3.16.9 Ringer File . . . . . 233
3.16.9.1 FTP/HTTPS Access Data . . . . . 234
3.16.9.2 Download Ringer File . . . . . 236
3.16.10 Dongle Key . . . . . 237
3.16.10.1 FTP/HTTPS Access Data . . . . . 237
3.16.10.2 Download Dongle Key File . . . . . 239
3.17 Corporate Phonebook: Directory Settings . . . . . 240
3.17.1 LDAP . . . . . 240
3.18 Speech . . . . . 242

3.18.1 RTP Base Port . . . . . 242
3.18.2 Codec Preferences . . . . . 243
3.18.3 Audio Settings . . . . . 245
3.19 Applications . . . . . 246
3.19.1 XML Applications/Xpressions (OpenStage 60/80) . . . . . 246
3.19.1.1 Setup/Configuration . . . . . 246
3.19.1.2 HTTP Proxy . . . . . 252
3.19.1.3 Modify an Existing Application . . . . . 254
3.19.1.4 Remove an Existing Application . . . . . 255
3.19.1.5 Application Start by Programmable Key . . . . . 255
3.20 Password . . . . . 256
3.21 Troubleshooting: Lost Password . . . . . 257
3.22 Restart Phone . . . . . 257
3.23 Factory Reset . . . . . 257
3.24 SSH – Secure Shell Access . . . . . 258
3.25 Display License Information . . . . . 259
3.26 Diagnostics . . . . . 260
3.26.1 Display General Phone Information . . . . . 260
3.26.2 View Diagnostic Information . . . . . 261
3.26.3 User Access to Diagnostic Information . . . . . 263
3.26.4 Diagnostic Call . . . . . 263
3.26.5 LAN Monitoring . . . . . 265
3.26.6 LLDP-MED . . . . . 266
3.26.7 IP Tests . . . . . 268
3.26.8 Process and Memory Information . . . . . 269
3.26.9 Fault Trace Configuration . . . . . 271
3.26.10 EasyTrace Profiles . . . . . 278
3.26.10.1 Bluetooth Handsfree . . . . . 278
3.26.10.2 Bluetooth Headset . . . . . 279
3.26.10.3 Call Connection . . . . . 279
3.26.10.4 Call Log . . . . . 280
3.26.10.5 Call Recording . . . . . 280
3.26.10.6 DAS Connection . . . . . 281
3.26.10.7 DLS Data Errors . . . . . 281
3.26.10.8 Help Application . . . . . 282
3.26.10.9 Key Input . . . . . 282
3.26.10.10 LAN Connectivity . . . . . 283
3.26.10.11 Messaging . . . . . 283
3.26.10.12 Mobility . . . . . 284
3.26.10.13 Phone administration . . . . . 284
3.26.10.14 LDAP Phonebook . . . . . 285
3.26.10.15 Local Phonebook . . . . . 285
3.26.10.16 Server based applications . . . . . 286
3.26.10.17 Sidecar . . . . . 286

3.26.10.18 SIP standard multiline . . . 287
3.26.10.19 SIP standard singleline . . . 287
3.26.10.20 Speech . . . 288
3.26.10.21 Tone . . . 288
3.26.10.22 USB Backup/Restore . . . 289
3.26.10.23 Voice Dialling . . . 289
3.26.10.24 Web Based Management . . . 290
3.26.10.25 802.1x problems . . . 290
3.26.10.26 No Tracing for All Services . . . 291
3.26.11 Bluetooth Advanced Traces . . . 292
3.26.12 QoS Reports . . . 293
3.26.12.1 Conditions and Thresholds for Report Generation . . . 293
3.26.12.2 View Report . . . 296
3.26.13 Core dump . . . 300
3.26.14 Remote Tracing – Syslog . . . 301
3.26.15 HPT Interface (For Service Staff) . . . 302
3.27 Bluetooth (OpenStage 60/80) . . . 303
3.28 MWI LED . . . 305
3.29 Missed Call LED . . . 307
3.30 Impact Level Notification . . . 308

**4 Technical Reference . . . 311**
4.1 Menus . . . 311
4.1.1 Web Interface Menu . . . 311
4.1.1.1 Menu Structure . . . 311
4.1.1.2 Web Pages . . . 315
4.1.2 Local Phone Menu . . . 360
4.2 Default Port List . . . 372
4.3 Troubleshooting: Error Codes . . . 374

**5 Examples and HowTos . . . 376**
5.1 Canonical Dialing . . . 376
5.1.1 Canonical Dialing Settings . . . 376
5.1.2 Canonical Dial Lookup . . . 377
5.1.2.1 Conversion examples . . . 378
5.2 How to Create Logo Files for OpenStage Phones . . . 380
5.2.1 For OpenStage 40 . . . 380
5.2.2 For OpenStage 60/80 . . . 381
5.3 How to Set Up the Corporate Phonebook (LDAP) . . . 384
5.3.1 Prerequisites . . . 384
5.3.2 Create an LDAP Template . . . 385
5.3.3 Load the LDAP Template onto the Phone . . . 389
5.3.4 Configure LDAP Access . . . 390
5.3.5 Test . . . 390
5.4 An LLDP-Med Example . . . 393

5.5 Dial Plan . . . . . 395
5.5.1 Introduction . . . . . 395
5.5.2 Dial Plan Syntax . . . . . 395
5.5.3 How To Set Up And Deploy A Dial Plan . . . . . 397
**Glossary . . . . . 401**
**Index . . . . . 408**

# 1 Overview

## 1.1 Important Notes

Do not operate the equipment in environments where there is a danger of explosions.

For safety reasons the phone should only be operating using the supplied plug in power unit.

Use only original accessories. The use of other accessories may be hazardous and will render the warranty, extended manufacturer's liability and the CE marking invalid.

Never open the telephone or add-on equipment. If you encounter any problems, contact System Support.

Installation requirement for USA, Canada, Norway, Finland and Sweden: Connection to networks which use outside cables is prohibited. Only in-house networks are permitted.

For USA and Canada only:
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This product is a UL Listed Accessory, I.T.E., in U.S.A. and Canada.
This equipment also complies with the Part 68 of the FCC Rules and the Industrie Canada CS-03.

## 1.2 Maintenance Notes

Do not operate the telephone in environments where there is a danger of explosions.

Use only original accessories from Siemens Enterprise Communications GmbH & Co. KG. Using other accessories may be dangerous, and will invalidate the warranty and the CE mark.

Never open the telephone or a key module. If you encounter any problems, contact System Support.

## 1.3 About the Manual

The instructions within this manual will help you in administering and maintaining the OpenStage phone. The instructions contain important information for safe and proper operation of the phones. Follow them carefully to avoid improper operation and get the most out of your multi-function telephone in a network environment.

This guide is intended for service providers and network administrators who administer VoIP services using the OpenStage phone and who have a fundamental understanding of VoIP, SIP, and IP networking. The tasks described in this guide are not intended for end users. Many of these tasks affect the ability of a phone to function on the network and require an understanding of IP networking and telephony concepts.

These instructions are laid out in a user-oriented manner, which means that you are led through the functions of the OpenStage phone step by step, wherever expedient. For the users, a separate manual is provided.

You can find further information on the official Unify website (http://www.unify.com/.) and on the Unify Wiki (http://wiki.unify.com/.).

## 1.4 Conventions for this Document

The terms for parameters and functions used in this document are derived from the web interface (WBM). In some cases, the phone's local menu uses shorter, less specific terms and abbreviations. In a few cases the terminologies differ in wording. If so, the local menu term is added with a preceding "/".

For the parameters described in this document, a WBM screenshot and the path in the local phone menu is provided. All WBM screenshots are taken from OpenStage 60/80. As some WBM input masks have been changed with firmware updates, the screenshots are selected after the following rules:

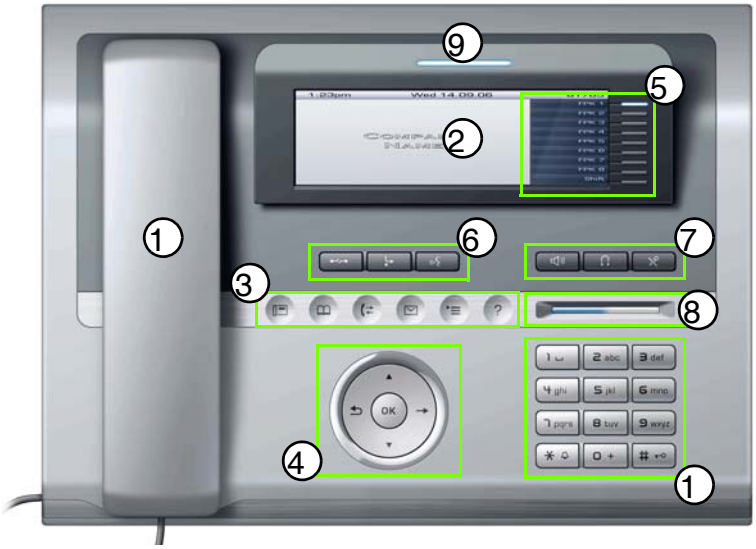
- If a later version contains more or less parameters compared to previous software versions, the screenshot of the older version is shown.

- If the title of a mask (e.g. "Pixel saver" vs. "Energy saving") or the name of a parameter (e.g. "Time Zone" vs. "DST zone") has changed, the later version is shown.
- If a parameter has moved from one mask to another, both older and later versions are shown. The same is true for the local menu paths.

This document describes the software version V3R3.

## 1.5 The OpenStage Family

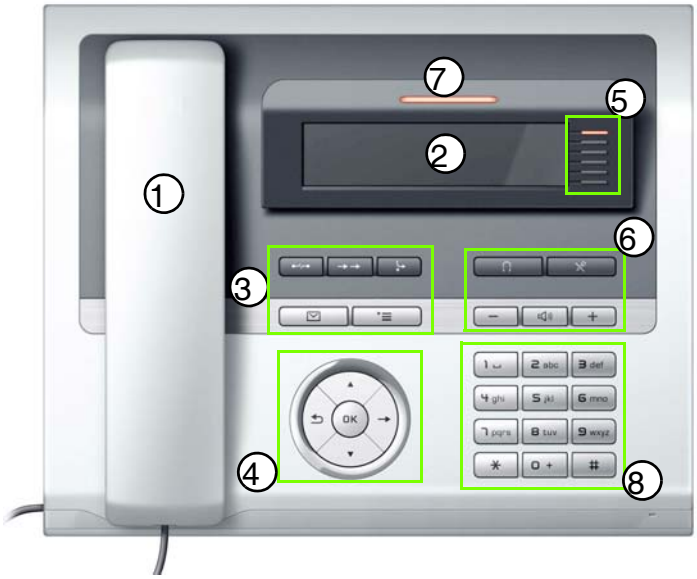
### 1.5.1 OpenStage 60/80




| | |
|---|---|
| 1 | With the **handset**, the user can pick up and dial calls in the usual manner. |
| 2 | The **graphic display** provides intuitive support for telephone operation. |
| 3 | The **mode keys** provide easy access to the phone's applications. |
| 4 | With the **TouchGuide**, the user/administrator can navigate in the phone functions, applications, and configuration menus. |
| 5 | The **free programmable keys** enable the user to customize the telephone in line with his/her personal needs by assigning individual phone numbers and functions. |
| 6 | The **fixed function keys** provide access to frequently used telephony functions. |
| 7 | With the **audio keys**, the user can control the audio settings. |
| 8 | With the **TouchSlider**, the user can adjust the volume, e.g. of ringtones. |
| 9 | Inbound calls are visually signaled via the **alert bar**. |
| 10 | The **keypad** is used for entering phone numbers and text. |

Tabelle 1-1

### 1.5.2 OpenStage 40




| | |
|---|---|
| 1 | With the **handset**, the user can pick up and dial calls in the usual manner. |
| 2 | The **graphic display** provides intuitive support for telephone operation. |
| 3 | The **fixed function keys** provide access to frequently used telephony functions. |
| 4 | With the **5-way navigator**, the user/administrator can navigate in the various phone functions, applications, and configuration menus. |
| 5 | The **free programmable keys** enable the user to customize the telephone in line with his/her personal needs by assigning individual phone numbers and functions. |
| 6 | With the **audio keys**, the user can control the audio settings. |
| 7 | Inbound calls are visually signaled via the **alert bar**. |
| 8 | The **keypad** is used for entering phone numbers and text. |

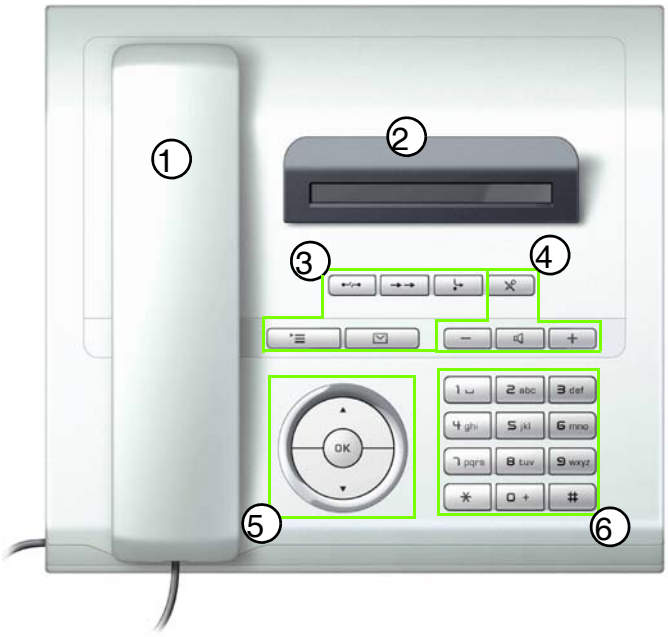
Tabelle 1-2

### 1.5.3 OpenStage 40 US

| | |
|---|---|
| 1 | With the **handset**, the user can pick up and dial calls in the usual manner. |
| 2 | The **graphic display** provides intuitive support for telephone operation. |
| 3 | The **fixed function keys** provide access to frequently used telephony functions. |
| 4 | With the **5-way navigator**, the user/administrator can navigate in the various phone functions, applications, and configuration menus. |
| 5 | The OpenStage 40 US telephone comes with six programmable lit sensor keys, preset to the following factory settings:<br>• Shift<br>• Phonebook<br>• Group pickup<br>• Call Forward<br>• DND<br>• Show phone<br>The user can customize the telephone with his/her personal needs by assigning individual phone numbers and functions. After a factory reset, the system will be reset to these values. |
| 6 | With the **audio keys**, the user can control the audio settings. |
| 7 | Inbound calls are visually signaled via the **alert bar**. |
| 8 | The **keypad** is used for entering phone numbers and text. |

Tabelle 1-3

## 1.5.4 OpenStage 20




| | |
|---|---|
| 1 | With the **handset**, the user can pick up and dial calls in the usual manner. |
| 2 | The **display** provides intuitive support for telephone operation. |
| 3 | The **fixed function keys** provide access to frequently used telephony functions. |
| 4 | With the **audio keys**, the user can control the audio settings. |
| 5 | With the **3-way navigator**, the user/administrator can navigate in the various phone functions, applications, and configuration menus. |
| 6 | The **keypad** is used for entering phone numbers and text. |

Tabelle 1-4

### 1.5.5 OpenStage 15

| | |
|---|---|
| 1 | With the **handset**, the user can pick up and dial calls in the usual manner. |
| 2 | The **display** provides intuitive support for telephone operation. |
| 3 | With the **audio keys**, the user can control the audio settings. |
| 4 | The **fixed function keys** provide access to frequently used telephony functions. |
| 5 | The **keypad** is used for entering phone numbers and text. |
| 6 | With the **navigation keys**, the user/administrator can navigate in the various phone functions, applications, and configuration menus. |
| 7 | The **free programmable keys** enable the user to customize the telephone in line with his/her personal needs by assigning individual phone numbers and functions. |

Tabelle 1-5

## 1.6 Administration Interfaces

You can configure the OpenStage phone by using any of the methods described in this chapter.

### 1.6.1 Web-based Management (WBM)

This method employs a web browser for communication with the phone via HTTPS. It is applicable for remote configuration of individual IP phones in your network. Direct access to the phone is not required.

To use this method, the phone must first obtain IP connectivity.

### 1.6.2 DLS (Deployment Service)

The Deployment Service (DLS) is an OpenScape Management application for administering phones and soft clients in communication networks. It has a Java-supported, web-based user interface, which runs on an internet browser. For further information, please refer to the Deployment Service Administration Guide.

### 1.6.3 Local Phone Menu

This method provides direct configuration of the OpenStage phone. Direct access to the phone is required.

As long as the IP connection is not properly configured, you have to use this method to set up the phone.

# 2 Startup

## 2.1 Prerequisites

The OpenStage phone acts as an endpoint client on an IP telephony network, and has the following network requirements:

- An Ethernet connection to a network with SIP clients and servers.

> ⚠ Only use **switches** in the LAN to which the OpenStage phone is connected. An operation at hubs can cause serious malfunctions in the hub and in the whole network.

- Phone Administration server.
- An FTP Server for file transfer, e. g. firmware, configuration data, application software.
- A DHCP (Dynamic Host Configuration Protocol) server (recommended).
- DLS (Deployment Service) for advanced configuration and software deployment (recommended).

For additional information see : http://wiki.unify.com/wiki/IEEE_802.1x.

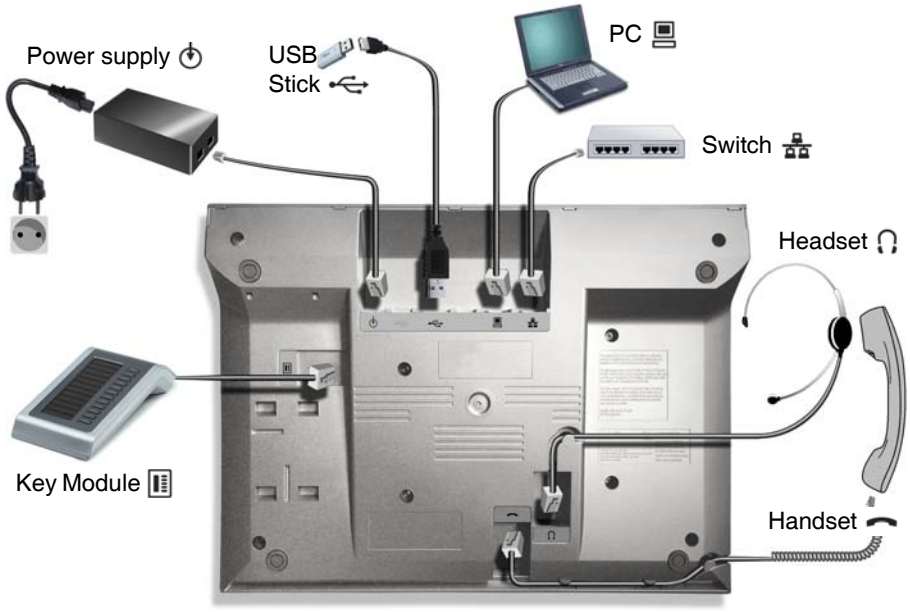
## 2.2 Assembling and Installing the Phone

### 2.2.1 Shipment

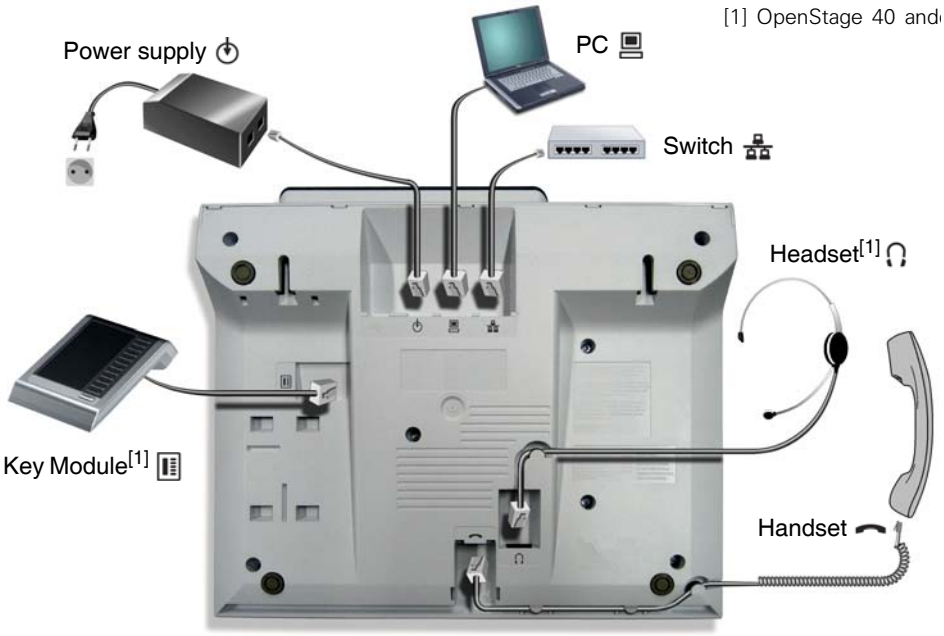
- **Phone**
- **Handset**
- **Handset cable**
- Subpackage:
  - **Document "Information and Important Operating Procedures"**
  - **Emergency number sticker**

### 2.2.2 Connectors at the bottom side

**OpenStage 60**



**OpenStage 40 (OpenStage 15 and 20 similar, except [1])**




## 2.2.3 Assembly

**1. Handset**

Insert the plug on the long end of the handset cable into the jack on the base of the telephone and press the cable into the groove provided for it. Next, insert the plug on the short end of the handset cable into the jack on the handset.

**2. Emergency Number Sticker**

Write your telephone number and those for the fire and police departments on the included label and attach it to the telephone housing underneath the handset (see arrow).

## 2.2.4 Connecting the Phone

1. Plug the LAN cable into the connector at the bottom of the telephone and connect the cable to the LAN resp. switch. If PoE (Power over Ethernet) is to be used, the PSE (Power Sourcing Equipment) must meet the IEEE 802.3af specification.
   For details about the required power supply, see the following table:

| Model | Power Consumption/Supply |
|---|---|
| OpenStage 15[1] | Power Class 1 |
| OpenStage 15 G[1] | Power Class 2 |
| OpenStage 20 E | Power Class 1 |
| OpenStage 20 | Power Class 1 |
| OpenStage 20 G | Power Class 2 |
| OpenStage 40[2], OpenStage 40 US[2] | Power Class 2 |
| OpenStage 40 + 2nd Key Module | Power Class 2 |
| OpenStage 40 G[2],OpenStage 40 G US[2] | Power Class 3 |
| OpenStage 40 G or OpenStage 40 G US + 2nd Key Module | Power Class 3 |
| OpenStage 60/80[3] | Power Class 3 |
| OpenStage 60/80 + 2nd Key Module | Power Class 3 |
| OpenStage 60/80 G[3] | Power Class 3 |
| OpenStage 60/80 G + 2nd Key Module | External power unit required |

1 Includes 1 Key Module 15.
2 Includes 1 Key Module.
3 Includes 1 Key Module + USB-Extension with Acoustic Unit.

2. Only if Power over Ethernet (PoE) is **NOT** supported:

> The order no. for the plug-in power supply is region specific:
> EU: C39280-Z4-C510
> UK: C39280-Z4-C512
> USA: C39280-Z4-C511

Plug the power supply unit into the mains. Connect the plug-in power supply unit to the jack at the bottom of the phone.

3. If applicable, connect the following optional jacks:
   - LAN connection to PC
   - Headset (accessory)
   - Connection to add-on device (accessory)
   - Connection to external keyboard (accessory)
   - USB master for connection to a USB device (e. g. accessory USB Acoustic Adapter)

> **To prevent damage on the OpenStage phone, connect an USB stick using the adapter cable C39195-Z7704-A5.**

> **Do not connect a USB hub to the phone's USB port, as this may lead to stability problems.**

## 2.3 Quick Start

This section describes a typical case: the setup of an OpenStage endpoint in an environment using a DHCP server and the web interface. For different scenarios, cross-references to the corresponding section of the administration chapter are given.

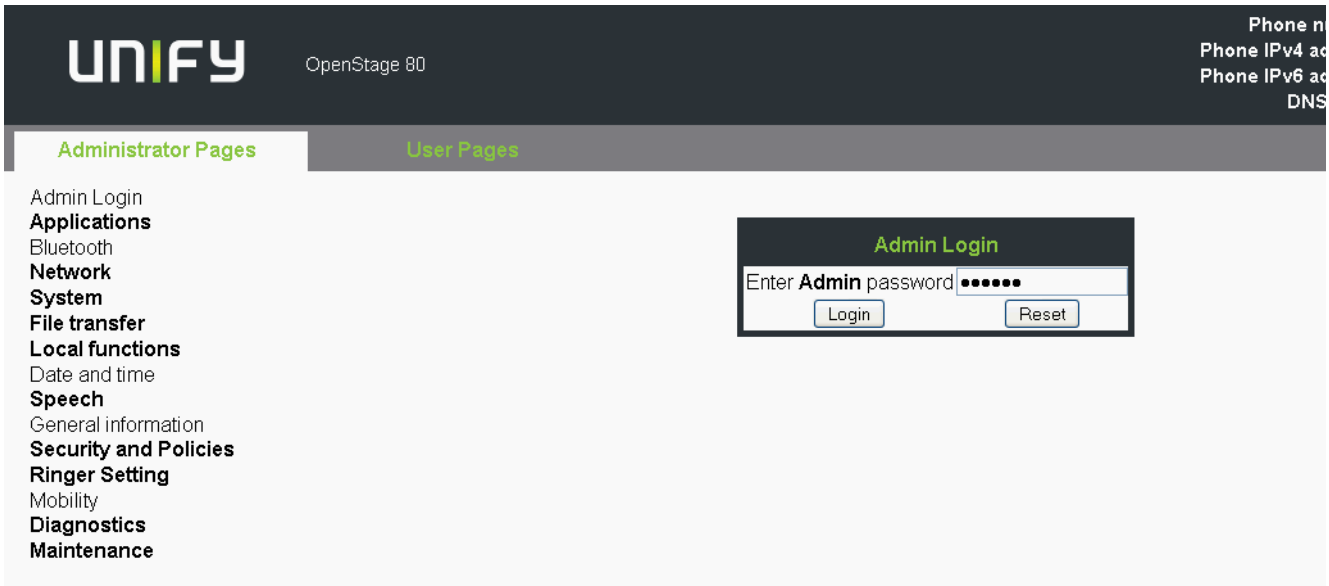
Alternatively, the DLS (Deployment Service) administration tool can be used. Its Plug & Play functionality allows to provide the phone with configuration data by assigning an existing data profile to the phone's MAC address or E.164 number. For further information, see the Deployment Service Administration Manual.

Any settings made by a DHCP server are not configurable by other configuration tools.

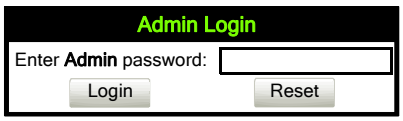
### 2.3.1 Accessing the Web Interface (WBM)

1. Open your web browser (MS Internet Explorer or Firefox) and enter the appropriate URL. Example: `https://192.168.1.15` or `https://myphone.phones`
   For configuring the phone's DNS name, please refer to Section 3.3.7.1, "DNS Domain Name".

   If the browser displays a certificate notification, accept it. The start page of the web interface appears. In the upper right corner, the phone number, the phone's IP address, as well as the DNS name assigned to the phone are displayed. The left corner contains the user menu tree.



2. Click on the tab "Administrator Pages". In the dialog box, enter the admin password:

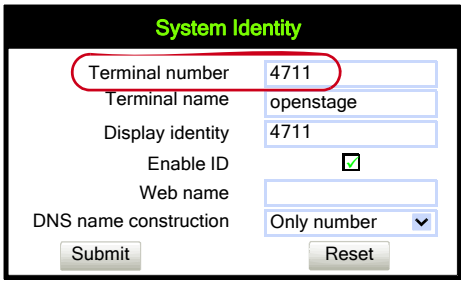



3. The administration main page opens. The left column contains the menu tree. If you click on an item which is printed in normal style, the corresponding dialog opens in the center of the page. If you click on an item printed in bold letters, a sub-menu opens in the right column.

## 2.3.2 Set the Terminal Number

If the user and administrator menus are needed in the course of setup, the terminal number, which by default is identical with the phone number, must be configured first. When the phone is in delivery status, the terminal number input form is presented to the user/administrator right after booting, unless the Plug&Play facility of the DLS is used. For further information about this setting, please refer to Section 3.5.1.1, “Terminal Identity”. With the WBM, the terminal number is configured as follows:

In the left column, select System > System Identity to open the "System Identity" dialog. Enter the terminal number, i. e. the SIP name / phone number.




## 2.3.3 Basic Network Configuration

For basic functionality, DHCP must provide the following parameters:

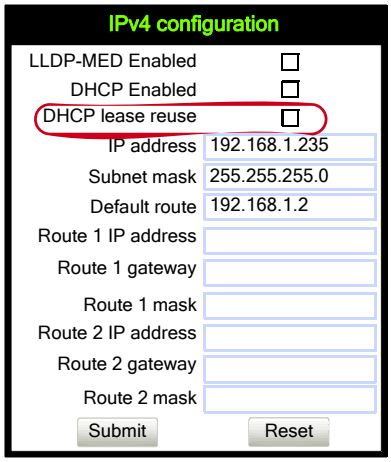
- **IP Address**: IP Address for the phone.
- **Subnet Mask (option #1)**: Subnet mask of the phone.
- **Default Route (option #3 "Router")**: IP Address of the default gateway which is used for connections beyond the subnet.
- **DNS IP Addresses (option #6 "Domain Server")**: IP Addresses of the primary and secondary DNS servers.

If no DHCP server is present, see Section 3.3.4, “IP Address - Manual Configuration” for IP address and subnet mask, and Section 3.3.5, “Default Route/Gateway” for the default route.

### 2.3.4 DHCP Resilience

It is possible to sustain network connectivity in case of DHCP server failure. If **DHCP lease reuse** is activated, the phone will keep its DHCP-based IP address even if the lease expires. To prevent address conflicts, the phone will send ARP requests in 5 second intervals. Additionally, it will send discovery messages periodically to obtain a new DHCP lease.

In the left column, select Network > IPv4 configuration to open the "System Identity" dialog. Select the check box to enable DHCP lease reuse.




### 2.3.5 Date and Time / SNTP

An SNTP (Simple Network Time Protocol) server provides the current date and time for network clients. The IP address of an SNTP server can be given by DHCP.

In order to provide the correct time, it is required to give the timezone offset, i.e. the shift in hours to be added to the UTC time provided by the SNTP server.

The following DHCP options are required:

- **SNTP IP Address (option #42 "NTP Servers")**: IP Address or hostname of the SNTP server to be used by the phone.
- **Timezone offset (option #2 "Time Offset")**: Offset in seconds in relationship to the UTC time provided by the SNTP server.

For manual configuration of date and time see Section 3.5.5, “Date and Time”.

### 2.3.6 SIP Server Address

The IP Address or hostname of the SIP server can be provided by DHCP.

The option's name and code are as follows:

- **option #120 "SIP Servers DHCP Option"**

For manual configuration of the SIP server address see Section 3.5.6.1, "SIP Addresses".

### 2.3.7 Extended Network Configuration

To have constant access to other subnets, you can enter a total of two more network destinations. For each further domain/subnet you wish to use, first the IP address for the destination, and then that of the router must be given. The option's name and code are as follows:

- **option #33 "Static Routing Table"**

For manual configuration of specific/static routing see Section 3.3.6, "Specific IP Routing".

Also the DNS domain wherein the phone is located can be specified by DHCP. The option's name and code are as follows:

- **option #15 "Domain Name"**

For manual configuration of the DNS domain name see Section 3.3.7.1, "DNS Domain Name".

### 2.3.8 Vendor Specific: VLAN Discovery And DLS Address

The VLAN ID can also be configured by LLDP-MED (see Section 3.2.2.2, "Automatic VLAN discovery using DHCP").

If the phone is to be located in a VLAN (Virtual LAN), a VLAN ID must be assigned. In case the VLAN shall be provided by DHCP, **VLAN Discovery** must be set to "DHCP" (see Section 3.2.2.2, "Automatic VLAN discovery using DHCP").

If a DLS (Deployment Service) server is in use, its IP address must be provided. It is recommended to configure the DLS server address by DCHP, as this method enables full Plug & Play: having received the DLS address from DHCP, the phone will contact the DLS during startup. Provided that the DLS is configured appropriately, it will send all necessary configuration data to the phone. Additionally, this method is relevant to security, as it ensures the authenticity of the DLS server.

For manual configuration of the DLS server address see Section 3.3.8, "Configuration & Update Service (DLS)".

For the configuration of vendor-specific settings by DHCP, there are two alternative methods: 1) the use of a vendor class, or 2) the use of DHCP option 43.

### 2.3.8.1 Using a Vendor Class

It is recommended to define a vendor class on the DHCP server, thus enabling server and phone to exchange vendor-specific data exclusively. The data is disclosed from other clients.

In the following, the configuration of vendor classes is explained both for a Windows DHCP Server and for Unix/Linux.

#### Configuration of the Windows DHCP Server

For DHCP servers on a pre-SP2 Windows 2003 Server:

Windows 2003 Server contains a bug that prevents you from using the DHCP console to create an option with the ID 1 for a user-defined vendor class. Instead, this entry must be created with the `netsh` tool in the command line (DOS shell).

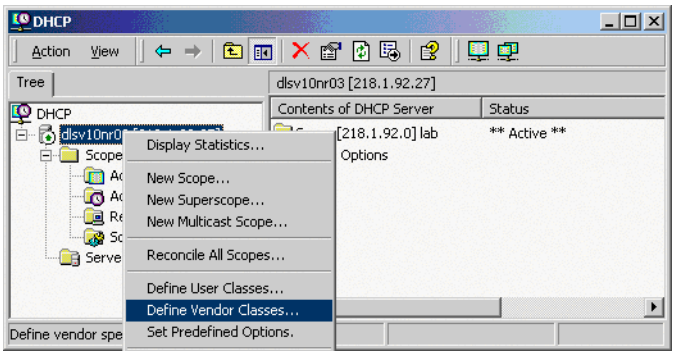
You can use the following command to set the required option (without error message), so that it will appear in the DHCP console afterwards:

```
netsh dhcp server add optiondef 1 "Optipoint element 001"
STRING 0 vendor=OptiIpPhone comment="Tag 001 for Optipoint"
```

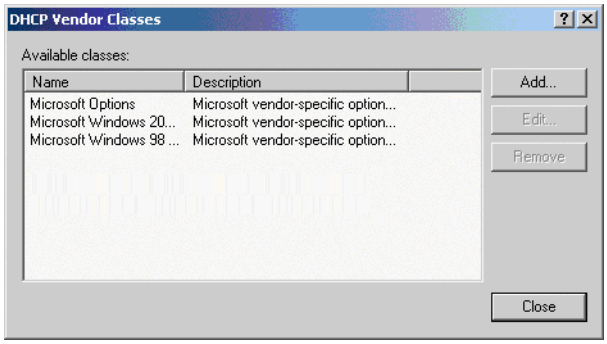
The value "Siemens" for optiPoint Element 1 can then be re-assigned using the DHCP console.

This error was corrected in Windows 2003 Server SP2.

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. In the DHCP console menu, right-click the DHCP server in question and select **Define Vendor Classes...** in the context menu.

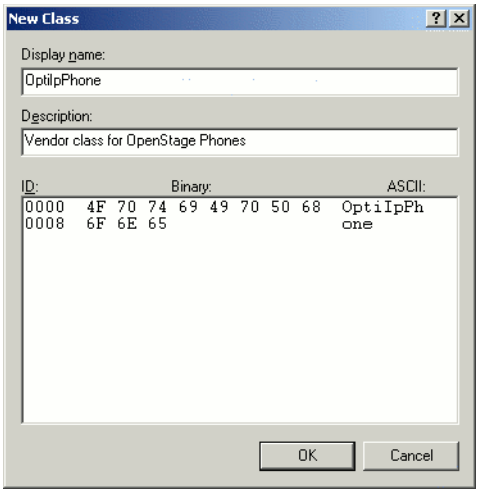



3. A dialog window opens with a list of the classes that are already available.

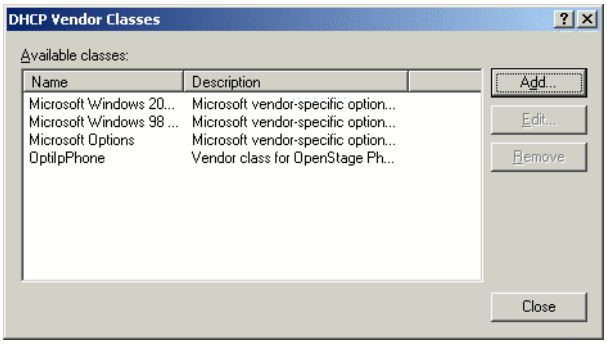



4. Press **Add...** to define a new vendor class.

5. Enter "OptiIpPhone" as **Display name** and give a description of this class. Provide the class name proper by setting the cursor underneath **ASCII** and typing "OptiIpPhone". The binary value is displayed simultaneously.

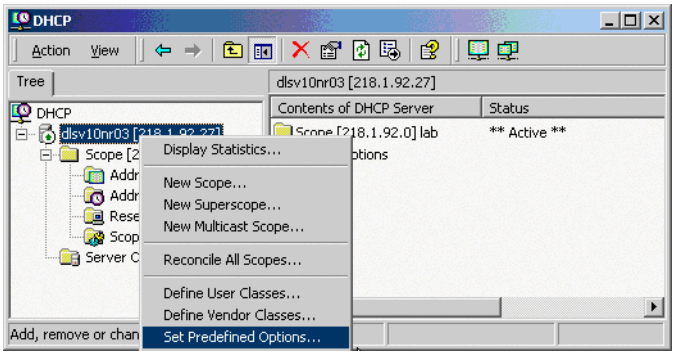



Click **OK** to apply the changes. The new vendor class now appears in the list:

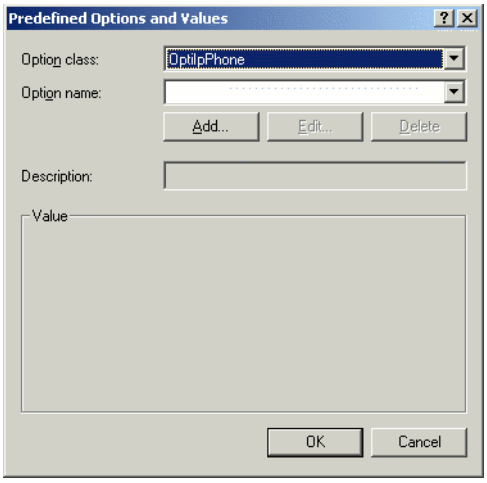



6. Exit the window with **Close**.

7. In the DHCP console menu, right-click the DHCP server in question and select **Set Predefined Options** from the context menu.

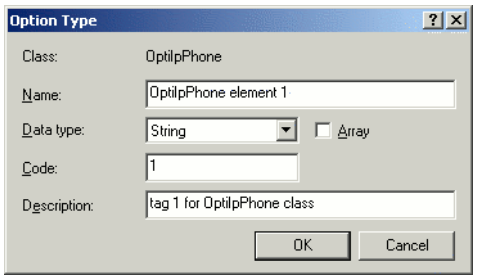



8. In the dialog, select the previously defined **OptiIpPhone** class and click on **Add...** to add a new option. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the first option will be there already.)



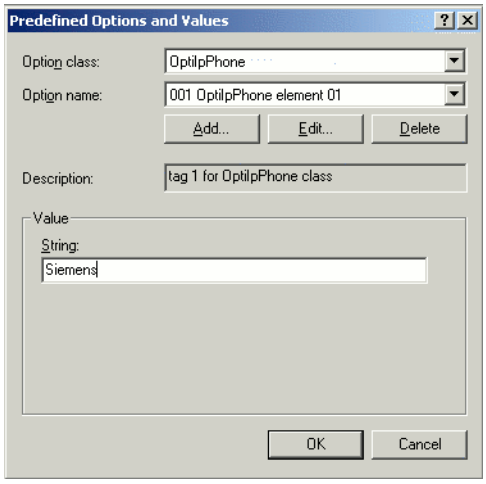
9. In the following dialog, specify the option type as follows. (If the workaround for a pre-SP2 Windows 2003 Server has been applied, the option type dialog will be skipped for the first option.)

   - **Name:** Free text, e. g. "OptiIpPhone element 01".
   - **Data type:** "String".
   - **Code:** "1".
   - **Description:** Free text, e. g. "tag 1 for OptiIpPhone class".




   Click **OK** to return to the previous window.

10. The newly created option is displayed now. Enter "Siemens" in the **Value** field.

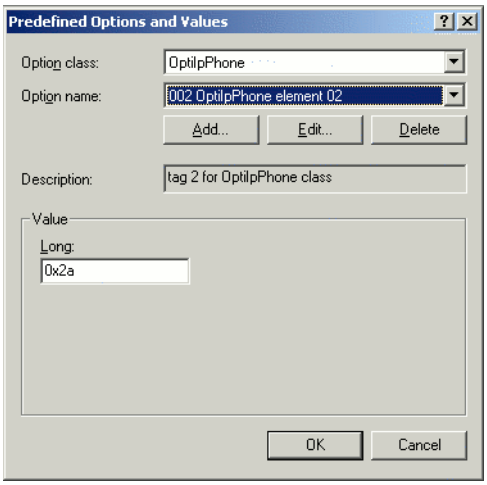


11. If the VLAN is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows. If you want to proceed to the configuration of the DLS address, continue with step 13.

    - **Name:** Free text, e. g. "OptiIpPhone element 02"
    - **Data type:** "Long"
    - **Code:** "2"
    - **Description:** Free text, e. g. "tag 2 for OptiIpPhone class".

    Click **OK** to return to the previous window.

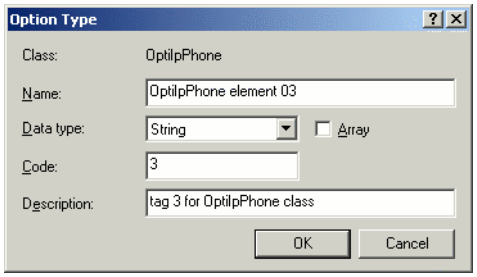
12. The newly created option is displayed now. Enter the VLAN ID as a hexadecimal number in the **Value** field. In the example, the VLAN ID is 10 (Hex: 2A).




    If you do not intend to configure the DLS address, click OK and continue with step 15.

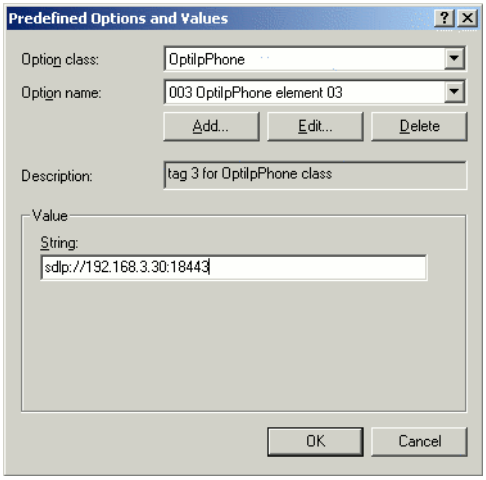
13. If the DLS address is to be provided by DHCP: Repeat step 7 and 8, and then specify the option type as follows.

    - **Name:** Free text, e. g. "OptiIpPhone element 03".
    - **Data type:** "String".
    - **Code:** "3"**.**
    - **Description:** Free text, e. g. "tag 3 for OptiIpPhone class".



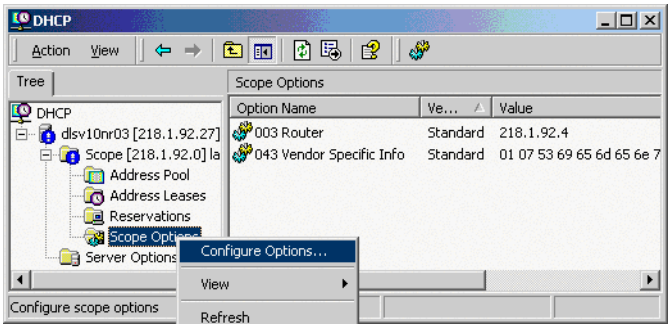

Click **OK** to return to the previous window.

14. The newly created option is displayed now. Enter the DLS address in the **Value** field, using the following format:
<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>
In the example, the DLS address is "sdlp://192.168.3.30:18443".

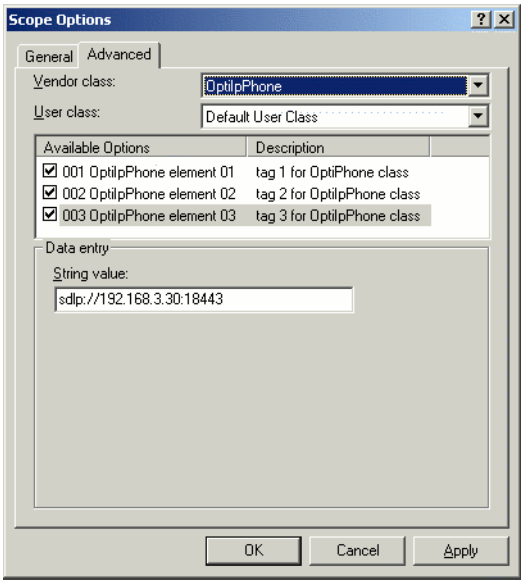



Click **OK**.

15. To define a scope, select the DHCP server in question, and then **Scope**, and right-click **Scope Options**. Select **Configure Options...** in the context menu.

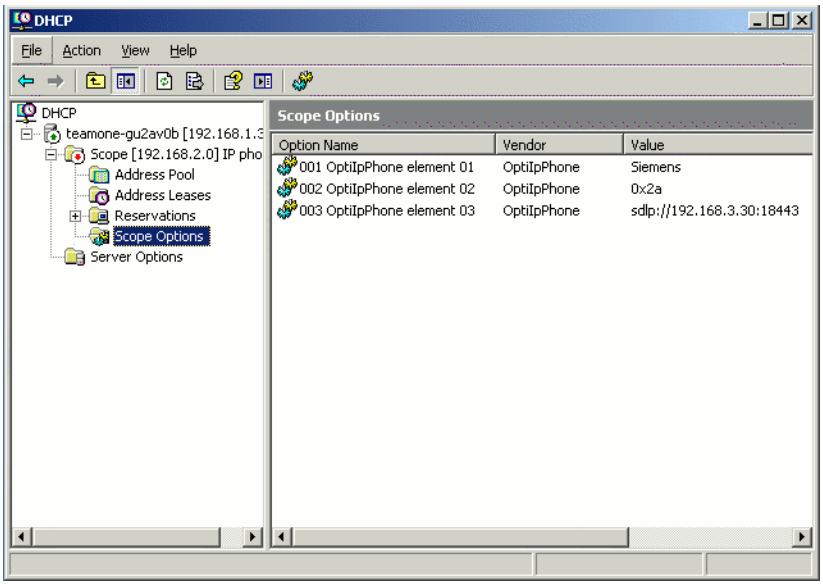



16. Select the **Advanced** tab. Under **Vendor class**, select the class that you previously defined (**OptiIpPhone**) and, under **User class**, select **Default User Class**.




Activate the check boxes for the options that you want to assign to the scope (in the example, **001**, **002**, and **003**). Click **OK**.

17. The DHCP console now shows the information that will be transmitted to the corresponding workpoints. Information from the **Standard** vendor is transmitted to all clients, whereas information from the **OptiIpPhone** vendor is transmitted only to the clients (workpoints) in this vendor class.



### Setup using a DHCP server on Unix/Linux

The following snippet from a DHCP configuration file (usually dhcpd.conf) shows how to set up a configuration using a vendor class and the "vendor-encapsulated-options" option.

```
class "OptiIpPhone" {
   option vendor-encapsulated-options
   # The vendor encapsulated options consist of hexadecimal values for
the option number (for instance, 01), the length of the value (for in-
stance, 07), and the value (for instance, 53:69:65:6D:65:6E:73). The
options can be written in separate lines; the last option must be fol-
lowed by a ';' instead of a ':'.
   # Tag/Option #1: Vendor must be "Siemens"
   #1  7  S  i  e  m  e  n  s
    01:07:53:69:65:6D:65:6E:73:
   # Tag/Option #2: VLAN ID
   # 2  4  0  0  0 10
    02:04:00:00:00:0A;
   # Tag/Option #3: DLS IP Address (here: sdlp://192.168.3.30:18443)
   # 3 25 s  d  l  p  :  / /  1  9  2  .  1  6  8  .  3  . (...etc.)
    03:19:73:64:6C:70:3A:2F:2F:31:39:32:2E:31:36:38:2E:33:2E:33:30:
3A:31:38:34:34:33;
   match if substring (option vendor-class-identifier, 0, 11) =
   "OptiIpPhone";
}
```

#### 2.3.8.2 Using Option #43 "Vendor Specific"

Alternatively, option #43 can be used for setting up the VLAN ID and DLS address. The following tags are used:

- **Tag 1: Vendor name**
- **Tag 2: VLAN ID**
- **Tag 3: DLS address**

Optionally, the DLS address can be given in an alternative way:

- **Tag 4: DLS hostname**

The Vendor name tag is coded as follows (the first line indicates the ASCII values, the second line contains the hexadecimal values):

| **Code** | **Length** | **Vendor name** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1 | 7 | S | i | e | m | e | n | s |
| 01 | 07 | 53 | 69 | 65 | 6D | 65 | 6E | 73 |

The following example shows a VLAN ID with the decimal value "10". Providing:

| **Code** | **Length** | **VLAN ID** | | | |
|---|---|---|---|---|---|
| 2 | 4 | 0 | 0 | 1 | 0 |
| 02 | 04 | 00 | 00 | 00 | 0A |

For manual configuration of the VLAN ID see Section 3.2.2.3, “Manual configuration of a VLAN ID”.

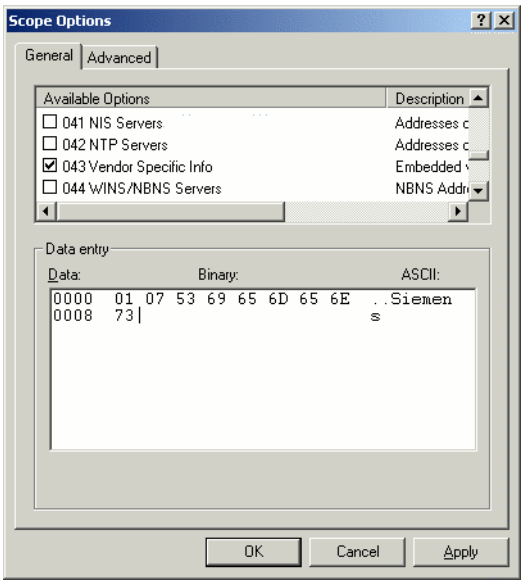
The DLS IP address tag consists of the protocol prefix "sdlp://", the IP address of the DLS server, and the DLS port number, which is "18443" by default. The following example illustrates the syntax:

| **Code** | **Length** | **DLS IP address** | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 25 | s | d | l | p | : | / | / | 1 | 9 | 2 | . | 1 | 6 | 8 | . | 3 | . | 3 | 0 | : | 1 | 8 | 4 | 4 | 3 |
| 03 | 19 | 73 | 64 | 6C | 70 | 3A | 2F | 2F | 31 | 39 | 32 | 2E | 31 | 36 | 38 | 2E | 33 | 2E | 33 | 30 | 3A | 31 | 38 | 34 | 34 | 33 |

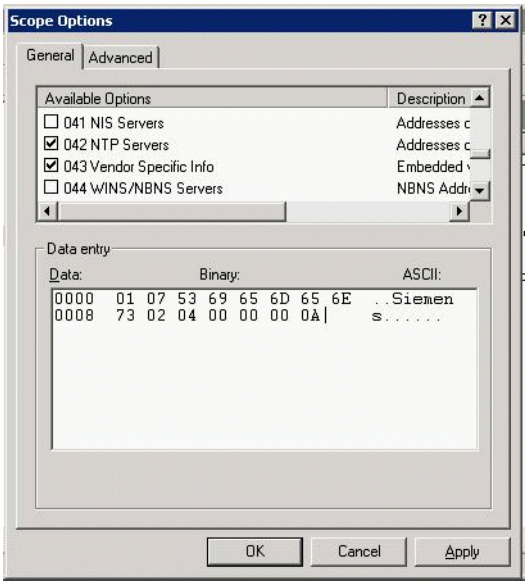
### Setup using the Windows DHCP Server

1. In the Windows Start menu, select **Start** > **Programs** > **Administrative Tools** > **DHCP**.
2. Select the DHCP server and the scope. Choose **Configure Options** in the context menu using the right mouse button.

3. Enter tag 1, that is the vendor tag. The value has to be "Siemens".



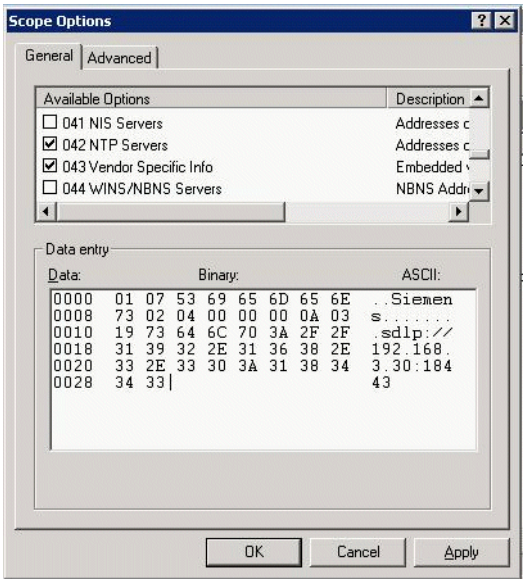

4. If the VLAN ID is to be provided by DHCP: Enter the hexadecimal value in **Data entry**. In the example, the VLAN ID is 10 (Hex: 0A).



5. If the DLS address is to be provided by DHCP: Enter the DLS address in the **Value** field, using the following format:
<PROTOCOL>:://<IP ADDRESS OF DLS SERVER>:<PORT NUMBER>

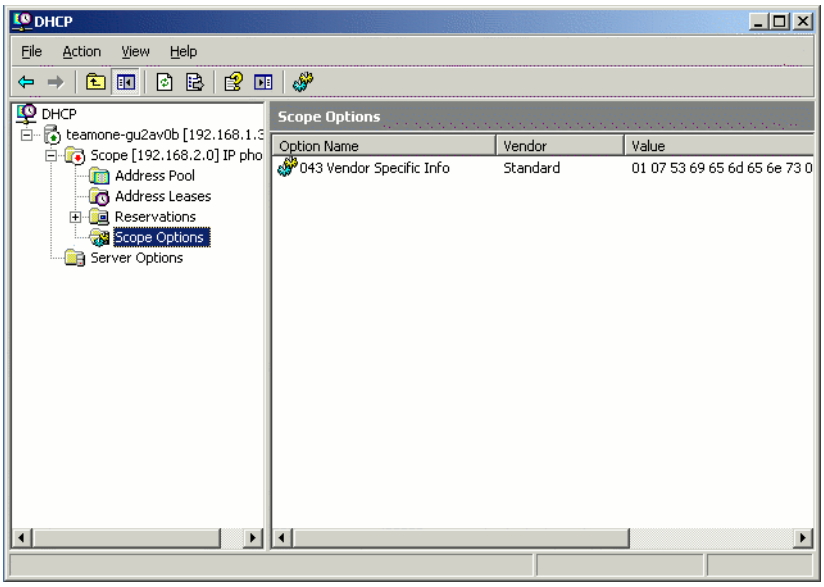
> For ensuring proper functionality, the port number should not be followed by any character.

In the example, the DLS address is "sdlp://192.168.3.30:18443".
Note that the screenshot also shows the VLAN ID described in step 4.




Click **OK**.

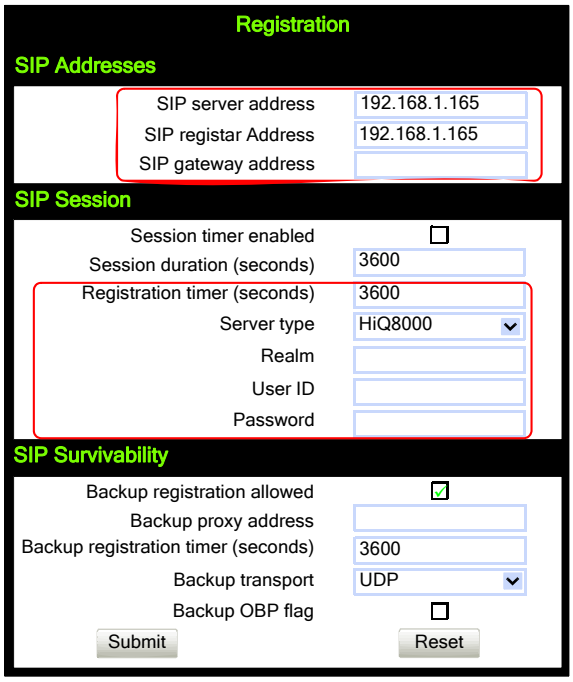
6. The DHCP console now shows the information that will be transmitted to the corresponding workpoints.



## 2.3.9 Registering at Phone Administration

For registration at the OpenStage SIP V3R3 SIP server, a SIP user ID and password must be provided by the phone. The following procedure describes the configuration using the web interface (see Section 2.3.1, “Accessing the Web Interface (WBM)”; if the web interface is not applicable, please refer to Section 3.5.7, “Authenticated Registration”) for configuration via the local menu.

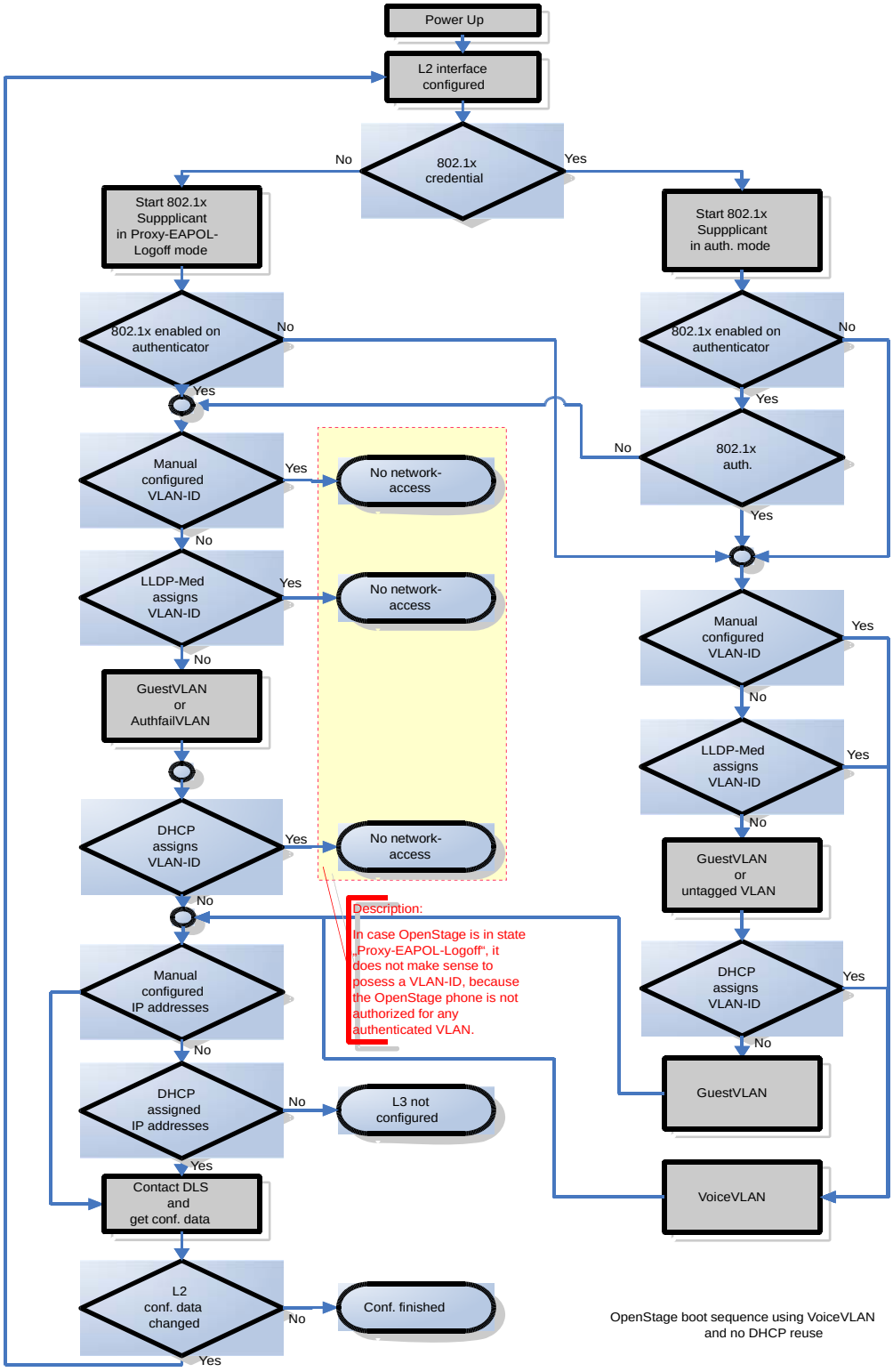
1. In the administration menu, select System > Registration. The **Registration** dialog opens.




2. Make sure that **SIP server address** and **SIP registrar address** contain the IP address of your OpenScape Voice server. If not provided by DHCP or DLS, enter the appropriate values. If the phone is to register with a gateway, enter the appropriate **SIP Gateway address**.
3. In the **Server type** field, select "OS Voice".
4. In **Realm**, enter the SIP realm the targeted user/password combination refers to.
5. In the **User ID** and **Password** fields, enter the user name/password combination for the phone.

## 2.4 Startup Procedure

The following flowchart shows the startup process for OpenStage phones:



## 2.5 Cloud Deployment

This chapter describes how a phone progresses through the cloud deployment process from factory start-up until the cloud service provider considers it to be ready for use by its User.

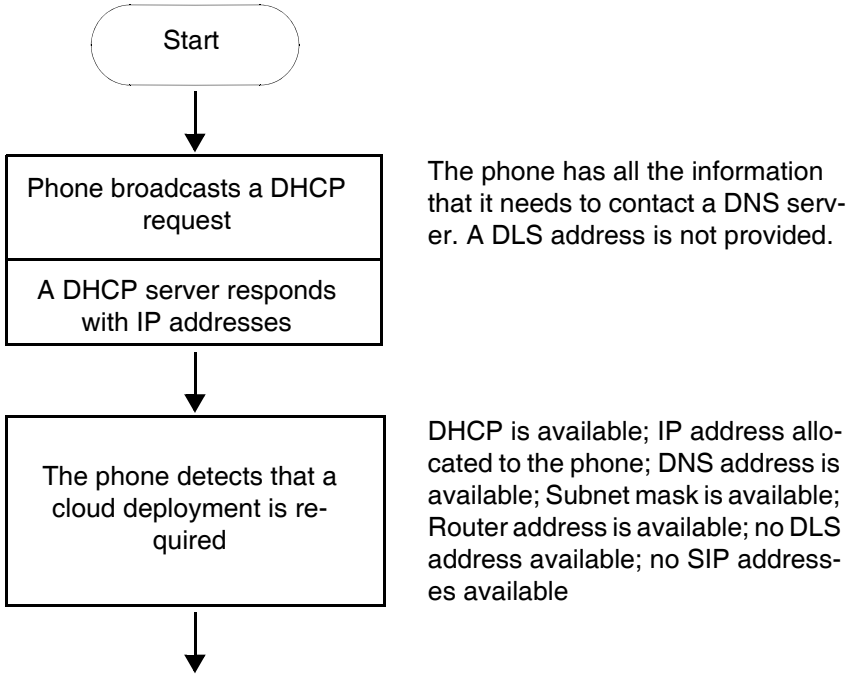
The phone determines that a cloud deployment process is to be used based on the IP settings it receives from the DHCP at the customer site. The Unify Redirect server[1] requires a code to determine which cloud service provider is responsible for the phone. The code is provided as part of a pin supplied from the cloud organisation to the User. When the User enters the pin at the phone the Unify Redirect server redirects the phone to a DLS-WPI based management system operated by the cloud service provider, This management system completes the configuration of the phone with all the information required for it to be usable and may also customise the phone for the cloud service provider's 'house' style.

### 2.5.1 Process of Cloud Deployment

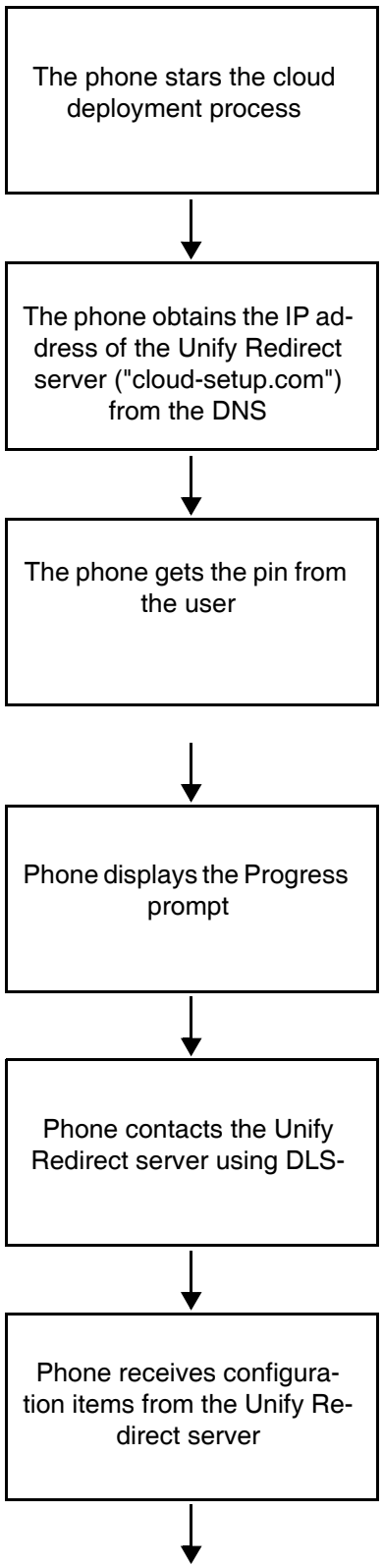
The following flow chart shows the way from a factory start-up until a user prepared OpenStage phone, deployed by a relevant DLS-WPI based management system.

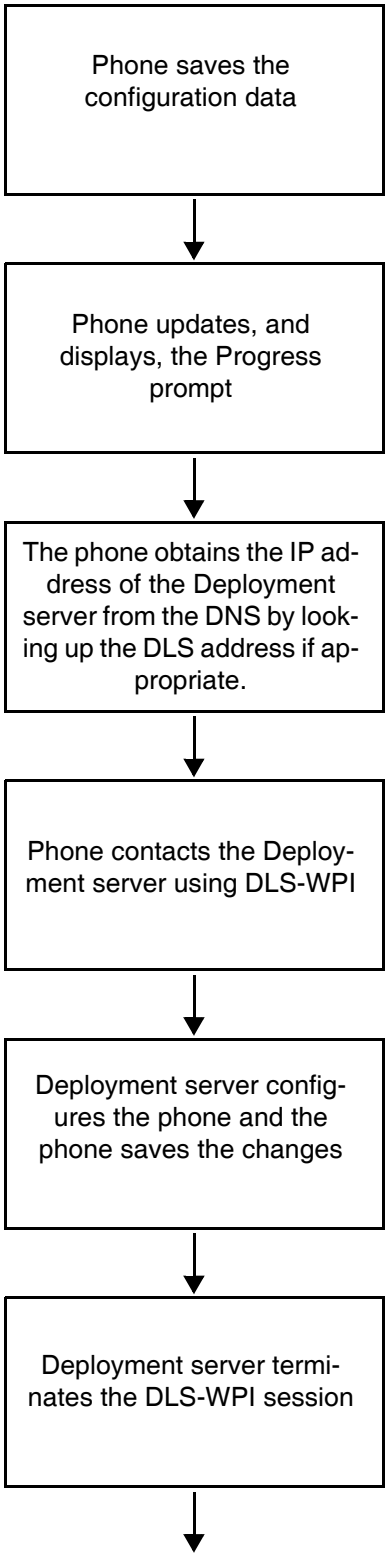
**Preconditions**:

- Phone is not running
- Phone is set to factory default values
- The phone has a LAN connection
- The LAN connection provides access to the public internet


Start
Phone broadcasts a DHCP request
A DHCP server responds with IP addresses
The phone has all the information that it needs to contact a DNS server. A DLS address is not provided.
The phone detects that a cloud deployment is required
DHCP is available; IP address allocated to the phone; DNS address is available; Subnet mask is available; Router address is available; no DLS address available; no SIP addresses available

1. The address for the Unify Redirect server is hardcoded as "'cloud-setup.com"

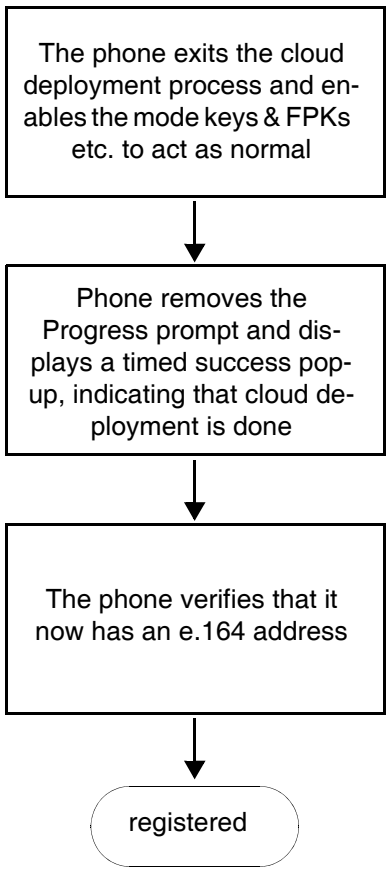

The phone stars the cloud deployment process
The phone is locked so that the mode keys & FPKs etc cannot be used
The phone obtains the IP address of the Unify Redirect server ("cloud-setup.com") from the DNS
The phone gets the pin from the user
The User enters the pin and presses **OK**. The phone verifies that the pin is valid.
The User has the option to **cancel** the process (see Kapitel 2, “Aborting cloud deployment process by User”
Phone displays the Progress prompt
Phone contacts the Unify Redirect server using DLS-
Phone receives configuration items from the Unify Redirect server
• DLS address (set to the name of the Deployment server)
• Language optional)
• DLS port (optional)


Phone saves the configuration data
Phone updates, and displays, the Progress prompt
The phone obtains the IP address of the Deployment server from the DNS by looking up the DLS address if appropriate.
Phone contacts the Deployment server using DLS-WPI
Deployment server configures the phone and the phone saves the changes
Deployment server terminates the DLS-WPI session

If the language is changed then the display is updated

The stored DLS address is not changed by the result of the DNS lookup

The hash of the pin is provided as an Inventory item to the Deployment server


The phone exits the cloud deployment process and enables the mode keys & FPKs etc. to act as normal
Phone removes the Progress prompt and displays a timed success pop-up, indicating that cloud deployment is done
The phone verifies that it now has an e.164 address
registered

## 2.5.2 Aborting cloud deployment process by User

The phone detects that a cloud deployment is required and starts the cloud deployment process. The Phone expects the input of the PIN by the User. At this point the User has the option to cancel the process with **Cancel**. If the User confirms his decision, the deployment process is aborted.

## 2.5.3 Re-trigger cloud deployment

Cloud deployment may be restarted by triggering a Factory reset:

The DLS-WPI requests a restart to factory defaults of the phone. The phone restart should then trigger the cloud deployment process.

### 2.5.4 Deployment errors

During deployment the display will always show deployment specific information. A persistent warning popup displays the information that will be shown in an idle screen error after deployment failed.

- It is shown to notify the phone User that deployment failed to complete as expected.
- It is a non-timed warning popup
- It is non-dismissible by user action
- It is shown over the idle screen only
- It is shown/re-shown whenever the idle screen is displayed or redisplayed to the user
- It is formatted as the warning icon followed by a warning text which ends in a code displayed in round brackets.
- The warning text is = "Deployment incomplete"
- It displays only the highest priority error condition should more than one error condition apply (note that priority 1 is the highest)

| Code | Priority | Cause |
|---|---|---|
| AU | 1 | Abandoned by user<br>Occurs when the pin prompt is dismissed |
| RS | 1 | Unable to get the address for the Unify Redirect server<br>DNS lookup failed |
| RN | 3 | Unable to establish contact with Unify Redirect server – no reply |
| RR | 2 | Unable to establish contact with Unify Redirect server – refused |
| RU | 1 | Unable to establish contact with Unify Redirect server - unauthorised |
| RO | 3 | Unable to establish contact with Unify Redirect server - no or invalid OCSP response |
| RV | 2 | Unable to establish contact with Unify Redirect server - certificate revoked |
| DS | 1 | Unable to get the address for the Deployment server<br>DNS lookup failed |
| DN | 3 | Unable to establish contact with Deployment server – no reply |
| DR | 2 | Unable to establish contact with Deployment server – refused |

# 3 Administration

This chapter describes the configuration of every parameter available on the OpenStage phones. For access via the local phone menu, see the following; for access using the web interface, please refer to Section 2.3.1, “Accessing the Web Interface (WBM)”.

## 3.1 Access via Local Phone

The data entered in input fields is parsed and controlled by the phone. Thus, data is accepted only if it complies to the value range.

1. **Access the Admin Menu**

   **OpenStage 60/80:**

   The menu key ☰ toggles between the Settings menu, the Applications menu, and the applications currently running. Press the ☰ key repeatedly until the "Settings" tab is active.

   **OpenStage 40:**

   Press the keys >☰, ▾, and OK consecutively to select **Settings > Admin** (the administration menu).

   **OpenStage 40 US:**

   Press the keys "Services", ▾, and OK consecutively to select **Settings > Admin** (the administration menu).

2. **Enter Password**

   When the Admin menu is active, you will be prompted to enter the administrator password. The default admin password is "123456". It is highly recommended to change the password (see Section 3.20, “Password”) after your first login.

   For entering passwords with non-numeric characters, please consider the following:

   By default, password entry is in numeric mode. For changing the mode, press the # key once or repeatedly, depending on the desired character. The # key cycles around the input modes as follows:

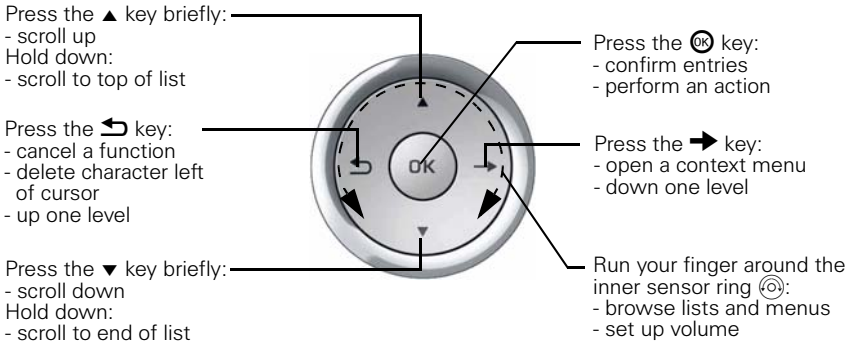
   (Abc) -> (abc) -> (123) -> (HEX) -> (ABC) -> back to start.

   Usable characters are 0-9 A-Z a-z .*#,?!’+-()@/:_

## 3. Navigate within the Admin Menu

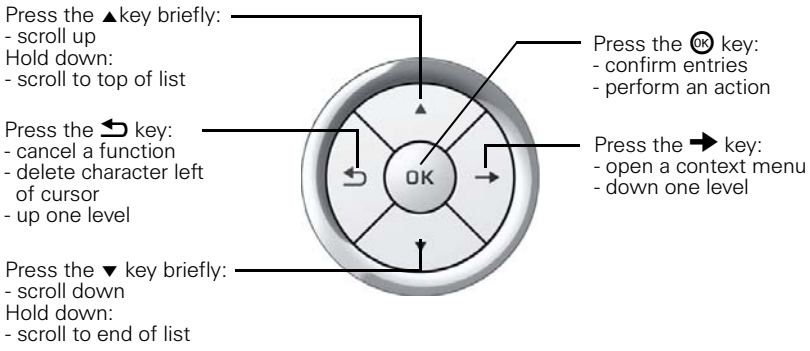
### OpenStage 60/80

Use the TouchGuide to navigate and execute administrative actions in the Admin menu.


Press the ▲ key briefly:
- scroll up
Hold down:
- scroll to top of list
Press the ⮌ key:
- cancel a function
- delete character left of cursor
- up one level
Press the ▼ key briefly:
- scroll down
Hold down:
- scroll to end of list
OK
Press the OK key:
- confirm entries
- perform an action
Press the ➔ key:
- open a context menu
- down one level
Run your finger around the inner sensor ring:
- browse lists and menus
- set up volume

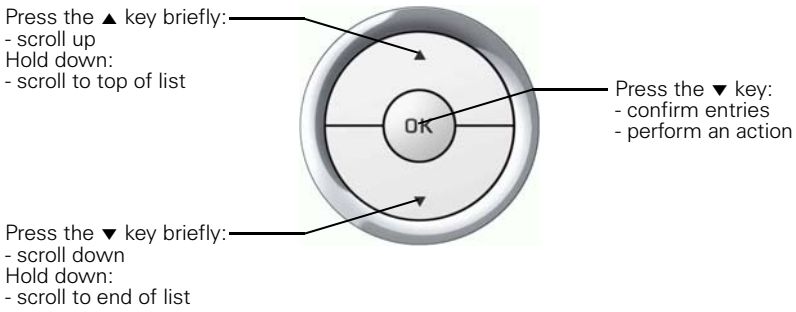
### OpenStage 40

Use the 5-way navigator to navigate and execute administrative actions in the administration menu.



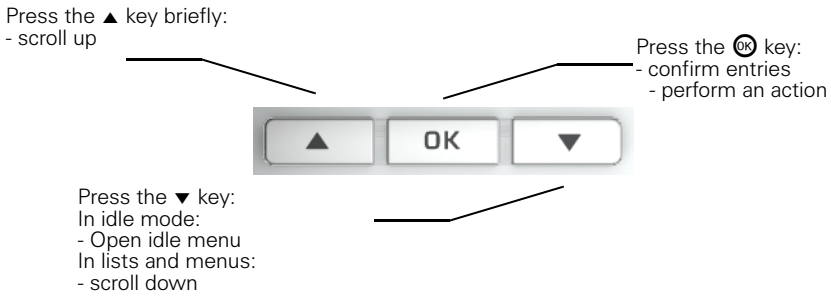
### OpenStage 20

Use the 3-way navigator to navigate and execute administrative actions in the administration menu.




### OpenStage 15

Use the navigation keys to navigate and execute administrative actions in the administration menu.




**4. Select a parameter**

If a parameter is set by choosing a value from a selective list, an arrow symbol appears in the parameter field that has the focus (on OpenStage 80,60, and 40 displays only). Press the OK key to enter the selective list. Use the Sensor Wheel resp. the ▲ and ▼ key to scroll up and down in the selective list. To select a list entry, press the OK key.

**5. Enter the parameter value**

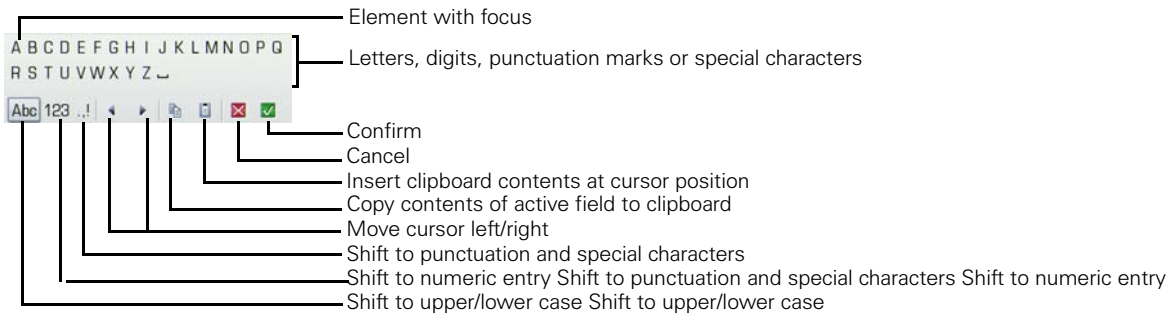
For selecting numbers and characters, you can use special keys. See the following table:

| Key | Function |
|---|---|
| * | Switch to punctuation and special characters. |
| # | Toggle between lowercase characters, uppercase characters, and digits in the following order:<br>(Abc) -> (abc) -> (123) -> (ABC) -> back to start. |

### OpenStage 60/80

If a parameter is set by entering a number or character data, the onscreen keypad is used. Press the OK key to enter the editor. Within the editor, solely use the key numbers or the Sensor Wheel for selecting numbers, characters, or groups of characters. The ⮌ key deletes one character in the input field, and the ➔ key moves the cursor to the OK field.

The following figure describes the elements of the onscreen keypad and their functions:


Element with focus
A B C D E F G H I J K L M N O P Q
R S T U V W X Y Z ␣
Abc 123 .!
Letters, digits, punctuation marks or special characters
Confirm
Cancel
Insert clipboard contents at cursor position
Copy contents of active field to clipboard
Move cursor left/right
Shift to punctuation and special characters
Shift to numeric entry Shift to punctuation and special characters Shift to numeric entry
Shift to upper/lower case Shift to upper/lower case

Additionally, you can use the following keys on the keypad as shortcuts for the selection of character groups

| Element | Function |
|---|---|
| * | Switch to punctuation and special characters. |
| # | Toggle between lowercase characters, uppercase characters, and digits. |

### OpenStage 15/20/40

With the OpenStage 15/20/40, use the keypad for entering parameters. With the 3 way/5 way navigator, you can enter, delete, copy, and paste characters and numbers as well as navigate within an entry and toggle the input mode.

### 6. Save and exit

When you are done, select **Save & exit** and press OK.

## 3.2 LAN Settings

### 3.2.1 LAN Port Settings

The OpenStage phone provides an integrated switch which connects the LAN, the phone itself and a PC port. By default, the switch will auto negotiate transfer rate (10/100 Mb/s, 1000 Mb/s with OpenStage 15/20/40/60/80 G) and duplex method (full or half duplex) with whatever equipment is connected. Optionally, the required transfer rate and duplex mode can be specified manually using the **LAN port speed** parameter.

In the default configuration, the LAN port supports automatic detection of cable configuration (pass through or crossover cable) and will reconfigure itself as needed to connect to the network.

The PC Ethernet port is controlled by the **PC port mode** parameter. If set to "Disabled", the PC port is inactive; if set to "Enabled", it is active. If set to "Mirror", the data traffic at the LAN port is mirrored at the PC port. This setting is for diagnostic purposes. If, for instance, a PC running Ethereal/Wireshark is connected to the PC port, all network activities at the phone's LAN port can be captured.

Removing the power from the phone, or a phone reset/reboot will result in the temporary loss of the network connection to the PC port.

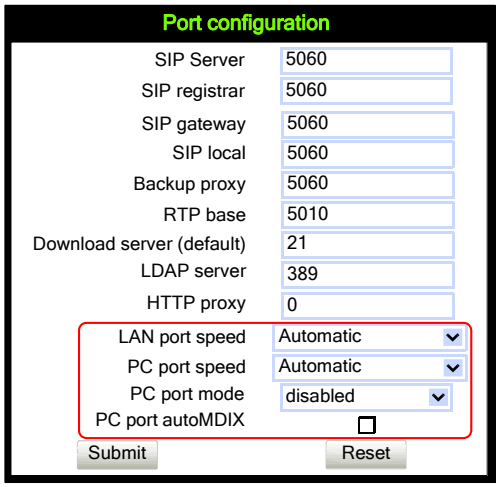
When **PC port autoMDIX** is enabled, the switch determines automatically whether a regular MDI connector or a MDI-X (crossover) connector is needed, and configures the connector accordingly.

**Data required**

- **LAN port speed** / **LAN port type**: Settings for the ethernet port connected to a LAN switch.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex".
  Default: "Automatic"
- **PC port speed** / **PC port type**: Settings for the ethernet port connected to a PC.
  Value range: "Automatic," "10 Mbps half duplex", "10 Mbps full duplex", "100 Mbps half duplex", "100 Mbps full duplex".
  Default: "Automatic"
- **PC port mode** / **PC port status**: Controls the PC port.
  Value range: "disabled", "enabled", "mirror".
  Default: "disabled"
- **PC port autoMDIX**: Switches between MDI and MDI-X automatically.
  Value range: "On", "Off"
  Default: "Off"

## Administration via WBM

Network > Port configuration




## Administration via Local Phone

- Admin
  - Network
    - Port Configuration
      - **LAN port type**
      - **PC port status**
      - **PC port type**
      - **PC port autoMDIX**

### 3.2.2 VLAN

VLAN (Virtual Local Area Network) is a technology that allows network administrators to partition one physical network into a set of virtual networks (or broadcast domains).

Partitioning a physical network into separate VLANs allows a network administrator to build a more robust network infrastructure. A good example is a separation of the data and voice networks into data and voice VLANs. This isolates the two networks and helps shield the endpoints within the voice network from disturbances in the data network and vice versa.

The implementation of a voice network based on VLANs requires the network infrastructure (the switch fabric) to support VLANs.

In a layer 1 VLAN, the ports of a VLAN-aware switch are assigned to a VLAN statically. The switch only forwards traffic to a particular port if that port is a member of the VLAN that the traffic is allocated to. Any device connected to a VLAN-assigned port is automatically a member of this VLAN, without being a VLAN aware device itself. If two or more network clients are connected to one port, they cannot be assigned to different VLANs. When a network client is moving from one switch to another, the switches' ports have to be updated accordingly by hand.

With a layer 2 VLAN, the assignment of VLANs to network clients is realized by the MAC addresses of the network devices. In some environments, the mapping of VLANs and MAC addresses can be stored and managed by a central database. Alternatively, the VLAN ID, which defines the VLAN whereof the device is a member, can be assigned directly to the device, e. g. by DHCP. The task of determining the VLAN for which an Ethernet packet is destined is carried out by VLAN tags within each Ethernet frame. As the MAC addresses are (more or less) wired to the devices, mobility does not require any administrator action, as opposed to layer 1 VLAN.

It is important that every switch connected to a PC is VLAN-capable. This is also true for the integrated switch of the OpenStage. The phone must be configured as a VLAN aware endpoint if the phone itself is a member of the voice VLAN, and the PC connected to the phone's PC port is a member of the data VLAN.

There are 3 ways for configuring the VLAN ID:

- Manually
- By DHCP
- By LLDP-MED

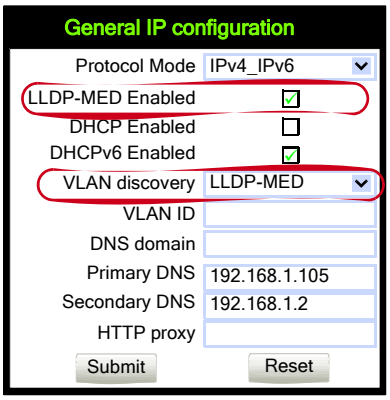
### 3.2.2.1 Automatic VLAN discovery using LLDP-MED

As an alternative, the VLAN ID can be configured by the network switch using LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery). If this option is selected, and the switch provides an appropriate TLV (Type-Length-Value) element containing the VLAN ID, this VLAN ID will be used. If no appropriate TLV is received, DHCP will be used for VLAN discovery.

#### Administration via WBM

Network > General IP configuration

To enable VLAN discovery via LLDP-MED, activate the **LLDP-MED Enabled** checkbox and select **LLDP-MED** in the **VLAN discovery** option. Afterwards, click **Submit**.




#### Administration via Local Phone

To enable VLAN discovery via LLDP-MED, set the **Use LLDP-MED** option to **Yes** and select **LLDP-MED** in the **VLAN discovery** option.

- Admin
  - Network
    - General IP configuration
      - Protocol mode
      - **Use LLDP-MED**
      - Use DHCP
      - Use DHCPv6
      - **VLAN discovery**
      - VLAN ID

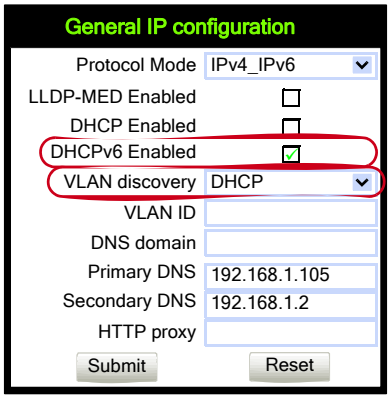
### 3.2.2.2 Automatic VLAN discovery using DHCP

To automatically discover a VLAN ID using DHCP, the phone must be configured as DHCP enabled, and **VLAN discovery** mode must be set to "DHCP". LLDP-MED should be disabled. The DHCP server must be configured to supply the Vendor Unique Option in the correct VLAN over DHCP format. If a phone configured for VLAN discovery by DHCP fails to discover its VLAN, it will proceed to configure itself from the DHCP within the non-tagged LAN. Under these circumstances, network routing may probably not be correct.

#### Administration via WBM

Network > General IP configuration

To enable VLAN discovery via DHCP, activate the **DHCPv6 Enabled** checkbox and select **DHCP** in the **VLAN discovery** option. Afterwards, click **Submit**.




#### Administration via Local Phone

To enable VLAN discovery via DHCP, activate the **DHCPv6 Enabled** checkbox and select **DHCP** in the **VLAN discovery** option.

- Admin
  - Network
    - General IP configuration
      - Protocol mode
      - Use LLDP-MED
      - Use DHCP
      - **Use DHCPv6**
      - **VLAN discovery**
      - VLAN ID

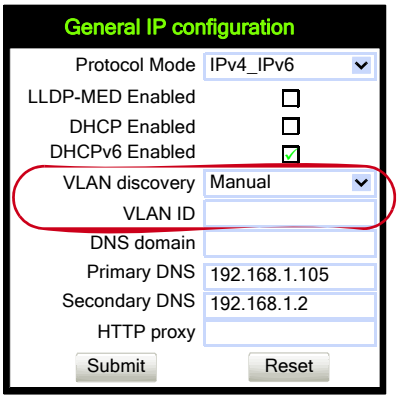
### 3.2.2.3 Manual configuration of a VLAN ID

To configure layer 2 VLAN manually, make sure that VLAN discovery is set to "Manual" and LLDP-MED is disabled. Then, the phone must be provided with a VLAN ID between 1 and 4095. If you mis-configure a phone to an incorrect VLAN, the phone will possibly not connect to the network. In DHCP mode it will behave as though the DHCP server cannot be found, in fixed IP mode no server connections will be possible.

#### Administration via WBM

Network > General IP configuration

The phone must be provided with a VLAN ID between 1 and 4095. Set the VLAN discovery to "Manual". Afterwards, click **Submit**.




#### Administration via Local Phone

```
└── Admin
    └── Network
        └── General IP Configuration
            └── VLAN ID
```

To enable VLAN discovery by Manual, select **Manual** in the **VLAN discovery** option.

```
└── Admin
    └── Network
        └── General IP configuration
            └── VLAN discovery
```

## 3.2.3 LLDP-MED Operation

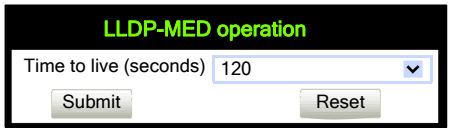
OpenStage phones support LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for auto-configuration and network management. The auto-configurable parameters are VLAN ID (see Section 3.2.2, “VLAN”) and Quality of Service parameters (see Section 3.3.1, “Quality of Service (QoS)”).

The data sent by a network device is stored in neighboring network devices in MIB (Management Information Base) format. In order to keep this information up-to-date, a specific TTL (Time To Live) is specified in LLDP. This value tells a device how long the received information is valid. For OpenStage phones, the value range is **40**, **60**, **80**, **100**, **110**, **120**, **140**, **180**, **240**, **320**, **400**.

An example for LLDP-MED operation an OpenStage phones can be found in Section 5.4, “An LLDP-Med Example”.

### Administration via WBM

Network > LLDP-MED operation




### Administration via Local Phone

```
└── Admin
    └── Network
        └── LLDP-MED operation
            ├── Extended power                    display only
            ├── Network policy (voice)            display only
            ├── LLDP-MED cap’s                    display only
            ├── MAC-Phy config                    display only
            ├── System Cap’s                      display only
            └── TTL
                └── TTL
```

## 3.3 IP Network Parameters

### 3.3.1 Quality of Service (QoS)

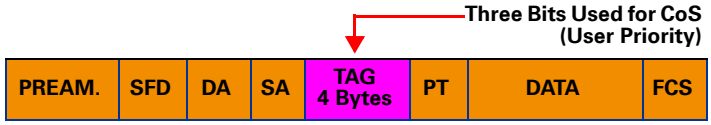
The QoS technology based on layer 2 and the two QoS technologies Diffserv and TOS/IP Precedence based on layer 3 are allowing the VoIP application to request and receive predictable service levels in terms of data throughput capacity (bandwidth), latency variations (jitter), and delay.

Layer 2 and 3 QoS for voice transmission can be set via LLDP-MED (see Section 3.26.6, “LLDP-MED”). If so, the value can not be changed by any other interface.

#### 3.3.1.1 Layer 2 / 802.1p

QoS on layer 2 is using 3 Bits in the 802.1q/p 4-Byte VLAN tag which has to be added in the Ethernet header.

The CoS (class of service) value can be set from 0 to 7. 7 is describing the highest priority and is reserved for network management. 5 is used for voice (RTP-streams) by default. 3 is used for signaling by default.

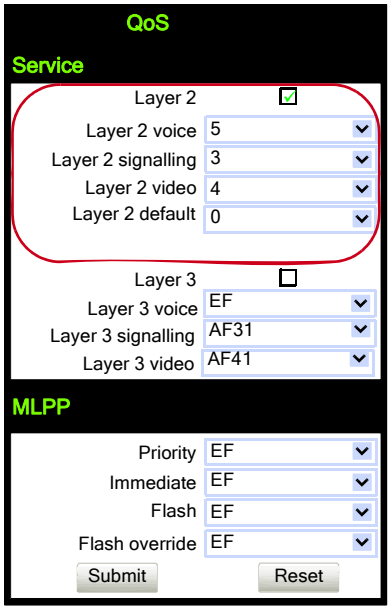



**Data required**

- **Layer 2**: Activates or deactivates QoS on layer 2.
  Value range: "Yes", "No"
  Default: "Yes"
- **Layer 2 voice**: Sets the CoS (Class of Service) value for voice data (RTP streams).
  Value range: 0-7
  Default: 5
- **Layer 2 signalling**: Sets the CoS (Class of Service) value for signaling.
  Value range: 0-7
  Default: 3
- **Layer 2 video**: Sets the CoS (Class of Service) value for video.
  Value range: 0-7
  Default: 4
- **Layer 2 default**: Sets the default CoS (Class of Service) value.
  Value range: 0-7
  Default: 0

### Administration via WBM

**Network** > QoS




### Administration via Local Phone

```
└--- Admin
     └--- Network
          └--- QoS
               └--- Service
                    |--- Layer 2
                    |--- Layer 2 voice
                    |--- Layer 2 signalling
                    |--- Layer 2 video
                    └--- Layer 2 default
```

### 3.3.1.2 Layer 3 / Diffserv

Diffserv assigns a class of service to an IP packet by adding an entry in the IP header.

Traffic flows are classified into 3 per-hop behavior groups:

1. Default
   Any traffic that does not meet the requirements of any of the other defined classes is placed in the default per-hop behaviour group. Typically, the forwarding has best-effort forwarding characteristics. The DSCP (Diffserv Codepoint) value for Default is "0 0 0 0 0 0".
2. Expedited Forwarding (EF referred to RFC 3246)

Expedited Forwarding is used for voice (RTP streams) by default. It effectively creates a special low-latency path in the network. The DSCP (Diffserv Codepoint) value for EF is "1 0 1 1 1 0".

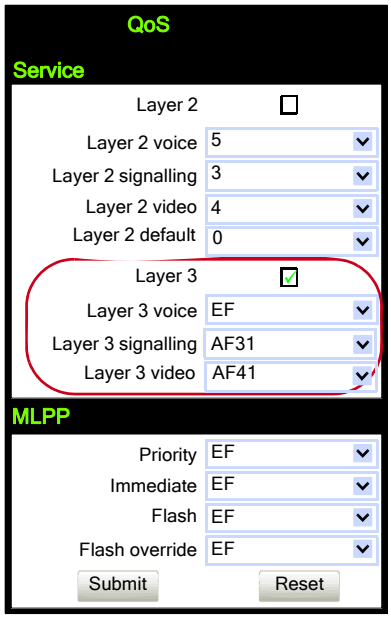
3. Assured Forwarding (AF referred to RFC 2597)
   Assured forwarding is used for signaling messages by default (AF31). It is less stringent than EF in a multiple dropping system. The AF values are containing two digits X and Y (AFXY), where X is describing the priority class and Y the drop level.
   Four classes X are reserved for AFXY: AF1Y (low priority), AF2Y, AF3Y and AF4Y (high priority).
   Three drop levels Y are reserved for AFXY: AFX1 (low drop probability), AFX2 and AFX3 (High drop probability). In the case of low drop level, packets are buffered over an extended period in the case of high drop level, packets are promptly rejected if they cannot be forwarded.

**Data required**

- **Layer 3**: Activates or deactivates QoS on layer 3.
  Value range: "Yes", "No"
  Default: "Yes"
- **Layer 3 voice**: Sets the CoS (Class of Service) value for voice data (RTP streams).
  Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
  Default: "EF"
- **Layer 3 signalling**: Sets the CoS (Class of Service) value for signaling.
  Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
  Default: "AF31"
- **Layer 3 video**: Sets the CoS (Class of Service) value for video.
  Value range: "BE", "AF11", "AF12", "AF13", "AF21", "AF22", "AF23", "AF31", "AF32", "AF33", "AF41", "AF42", "AF43", "EF", "CS7", "CS3", "CS4", "CS5", 0, 1, 2 ... through 63.
  Default: "AF41"

## Administration via WBM

Network > QoS




## Administration via Local Phone

```
└── Admin
    └── Network
        └── QoS
            └── Service
                ├── Layer 3
                ├── Layer 3 voice
                ├── Layer 3 signalling
                └── Layer 3 video
```

## 3.3.2 Protocol Mode IPv4/IPv6

An IPv4 address consists of 4 number blocks, each between 0 and 255, separated by ".".
Example:

1.222.44.123

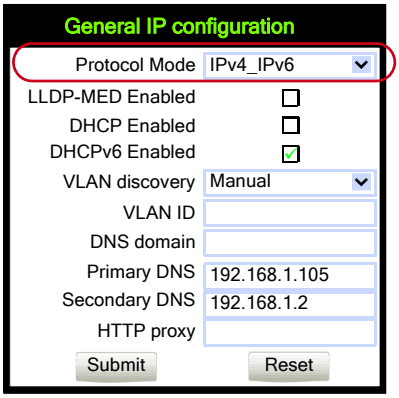
An IPv6 address consists of 8 hexadecimal number blocks, separated by ":".
Example:
2001:0db8:85a3:08d3:1319:8a2e:0370:7347 or, if not all blocks are used:

2000:1::3

### Administration via WBM

Network > General IP configuration

Set the **Protocol Mode** to "IPv4" or "IPv6" or both (the default setting is IPv4_IPv6). Afterwards, click **Submit**.




### Administration via Local Phone

Admin
Network
General IP Configuration
**Protocol Mode**

### 3.3.3 Use DHCP

If this parameter is set to "Yes" (default), the phone will search for a DHCP server on startup and try to obtain IP data and further configuration parameters from that central server.

If no DHCP server is available in the IP network, please deactivate this option. In this case, the IP address, subnet mask and default gateway/route must be defined manually.

The phone is able to maintain its IP connection even in case of DHCP server failure. For further information, please refer to Section 2.3.4, “DHCP Resilience”.

The following parameters can be obtained by DHCP:

**Basic Configuration**

- IP Address
- Subnet Mask

**Optional Configuration**

- Default Route (Routers option 3)
- IP Routing/Route 1 & 2 (Static Routes option 33, Classless static route option 121, Private/ Classless Static Route (Microsoft) option 249)
- SNTP IP Address (NTP Server option 42)
- Timezone offset (Time Server Offset option 2)
- Primary/Secondary DNS (DNS Server option 6)
- DNS Domain Name (DNS Domain option 15)
- SIP Addresses / SIP Server & Registrar (SIP Server option 120)
- VLAN ID, DLS address (Vendor specific Information option 43)

The following parameters can be obtained by DHCPv6:

**Basic Configuration**

- Global Address
- Global Address Prefix Length

**Optional Configuration**

- Primary/Secondary DNS (DNS recursive name server option 23)
- SNTP IP Address (Simple Network Time Protocol Server option 31)

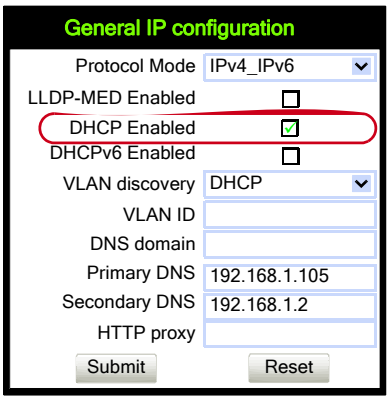
- SIP Addresses / SIP Server & Registrar (SIP Server Domain Name List option 21, SIP Server IPv6 Address List option 22)
- VLAN ID, DLS address (Vendor specific Information option 17)

DHCPv6 options are preferred in Dual Stack Mode if a parameter is configured both via DHCP and via DHCPv6, for instance DNS or SNTP server addresses.

### Administration via WBM

Network > General IP configuration

Set **DHCP Enabled** to selected. Afterwards, click **Submit**.




### Administration via Local Phone

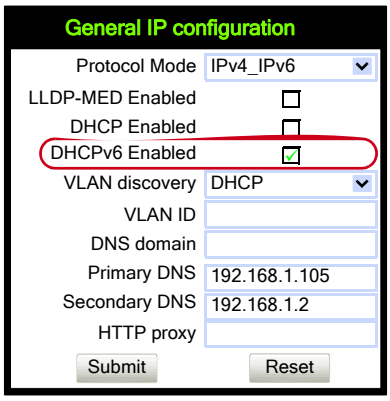
```
└── Admin
    └── Network
        └── IPv4 configuration
```

or/and

### Administration via WBM

Network > General IP configuration

Set **DHCPv6 Enabled** to selected (the default setting is **Enabled**). Afterwards, click **Submit**.




### Administration via Local Phone

└--- Admin
  └--- Network
    └--- **IPv6 configuration**

## 3.3.4 IP Address - Manual Configuration

### 3.3.4.1 Configuration

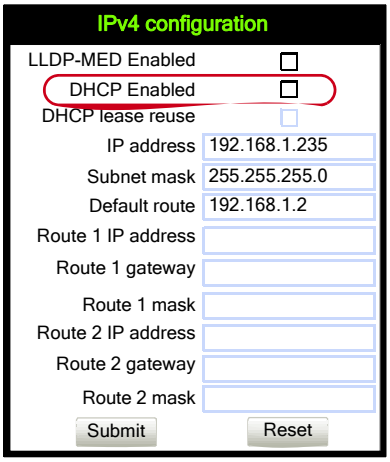
If not provided by DHCP dynamically, the phone's IP address and subnet mask must be specified manually.

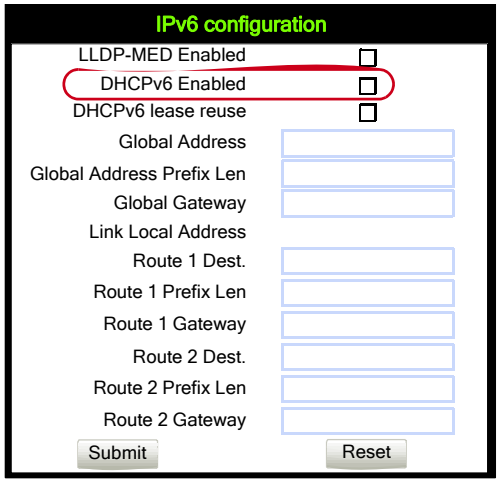
IP addresses can be entered in the following formats:

- Decimal format. Example: 11.22.33.44 or 255.255.255.0 (no leading zeroes).
- Octal format. Example: 011.022.033.044 (leading zeroes must be used with every address block)
- Hexadecimal format. Example: 0x11.0x22.0x33.0x44 (prefix 0x must be used with every address block)

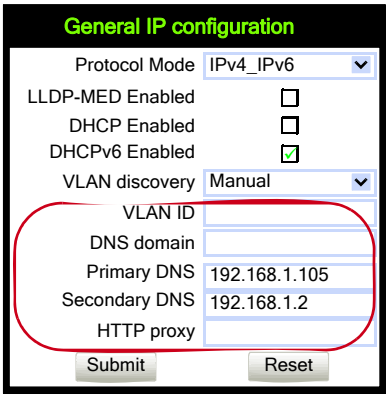
By default, IP configuration by DHCP and LLDP-MED is enabled. For manual IP configuration, please proceed as follows:

1. Navigate to **Network** > **General IP configuration**. Set **DHCP Enabled**, **DHCPv6 Enabled** and **LLDP-MED** to "not selected". Afterwards, click **Submit**.
2. Navigate to **Network** > **General IP configuration**> **IPv4 configuration** or **IPv6 configuration** depending on settings in Section 3.3.2, "Protocol Mode IPv4/IPv6". Enter the **IP address** and the **Subnet mask**. If applicable, enter the **Default route**. Afterwards, click **Submit**.




3. After the phone's network service has restarted, the other IP parameters can be configured.




## Administration via Local Phone

Admin
Network
General IP configuration
**Use LLDP-MED**
**Use DHCP**
**Use DHCPv6**

Admin
Network
IPv4 configuration
**IP address**
**Subnet mask**

Admin
Network
IPv4 configuration
**Global address**
**Global Prefix Len**

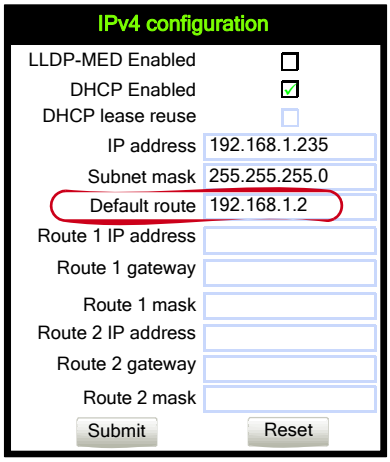
## 3.3.5 Default Route/Gateway

If not provided by DHCP dynamically (see Section 3.3.3, “Use DHCP”), enter the IP address of the router that links your IP network to other networks. If the value was assigned by DHCP, it can only be read.

### Administration via WBM

Network > IPv4 configuration

Enter the IP address of the router that links your IP network to other networks. Afterwards, click **Submit**.



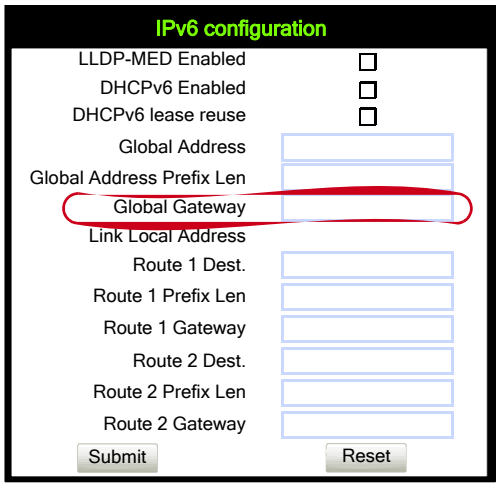

### Administration via Local Phone

└--- Admin
  └--- Network
    └--- **IPv4 configuration**
      └--- **Route (Default)**

## Administration via WBM

Network > IPv6 configuration

Enter the IP address of the Global Gateway that links your IP network to other networks. Afterwards, click **Submit**.




## Administration via Local Phone

└── Admin
  └── Network
    └── **IPv6 configuration**
      └── **Global Gateway**

## 3.3.6 Specific IP Routing

To have constant access to network subscribers of other domains, you can enter a total of two more network destinations, in addition to the default route/gateway. This is useful if the LAN has more than one router.

### IPv4 Route Configuration

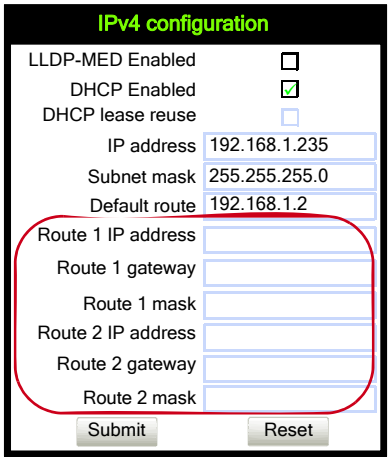
### Data required

- **Route 1/2 IP address**: IP address of the selected route.
- **Route 1/2 gateway**: IP address of the gateway for the selected route.
- **Route 1/2 mask**: Network mask for the selected route.

### Administration via WBM

Network > IPv4 configuration

Enter the IP address of the router that links your IP network to other networks. Click **Submit**.




### Administration via Local Phone

```
└── Admin
    └── Network
        └── IPv4 configuration
            ├── Route 1 IP
            ├── Route 1 gateway
            ├── Route 1 mask
            ├── Route 2 IP
            ├── Route 2 gateway
            └── Route 2 mask
```

## IPv6 Route Configuration

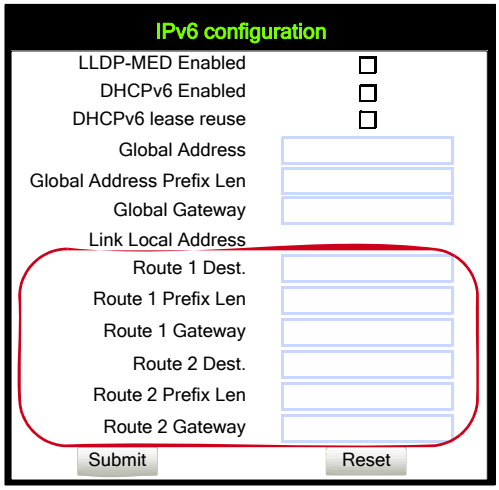
### Data required

- **Route 1/2 destination**: IPv6 address of the selected route.
- **Route 1/2 prefix len**: Prefix length for the selected route.
- **Route 1/2 gateway**: IPv6 address of the gateway for the selected route.

### Administration via WBM

Network > IPv6 configuration

Enter the IP address of the router that links your IP network to other networks. Afterwards, click **Submit**.




### Administration via Local Phone

```
└--- Admin
     └--- Network
          └--- IPv6 configuration
               |--- Route 1 dest
               |--- Route 1 prefix len
               |--- Route 1 gateway
               |--- Route 2 dest
               |--- Route 2 prefix len
               |--- Route 2 gateway
```

## 3.3.7 DNS

The main task of the domain name system (DNS) is to translate domain names to IP addresses. For some features and functions of the OpenStage phone, it is necessary to configure the DNS domain the phone belongs to, as well as the name servers needed for DNS resolving.

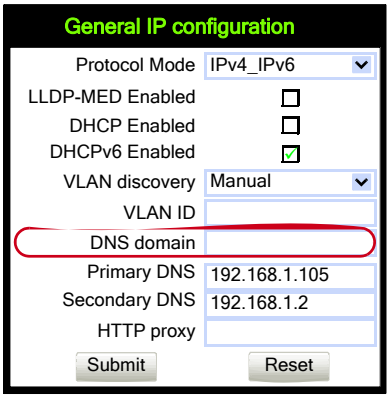
### 3.3.7.1 DNS Domain Name

This is the name of the phone's local domain.

#### Administration via WBM

Network > General IP configuration

Enter the DNS domain the phone belongs to. Afterwards, click **Submit**.




#### Administration via Local Phone

Admin
Network
**General IP configuration**
**DNS domain**

### 3.3.7.2 DNS Servers

If not provided by DHCP automatically, a primary and a secondary DNS server can be configured.

> Enhanced survivability using DNS SRV is available. To make use of it, a special configuration is required. For details, please refer to Section 3.5.10, “Resilience and Survivability”.

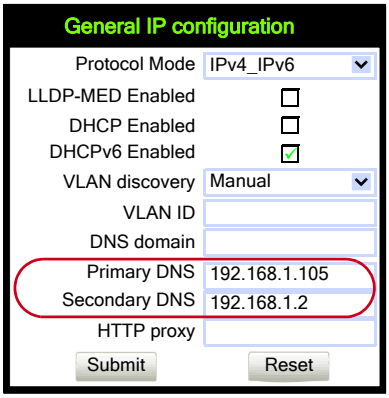
#### Data required

- **Primary DNS**: IP address of the primary DNS server.
- **Secondary DNS**: IP address of the secondary DNS server.

#### Administration via WBM

Network > General IP configuration

Enter the IP addresses of the primary and the secondary DNS server. Afterwards, click **Submit**.




#### Administration via Local Phone

```
└--- Admin
    └--- Network
        └--- General IP configuration
            |--- Primary DNS
            └--- Secondary DNS
```

### 3.3.7.3 Terminal Hostname

The phone's hostname  can be customized.

The corresponding DNS domain is configured in Network > IP configuration > DNS domain (see Section 3.3.7.1, "DNS Domain Name").

The current DNS name of the phone is displayed at the right-hand side of the banner of the admin and user web pages, under **DNS name**. To see configuration changes, the web page must be reloaded.

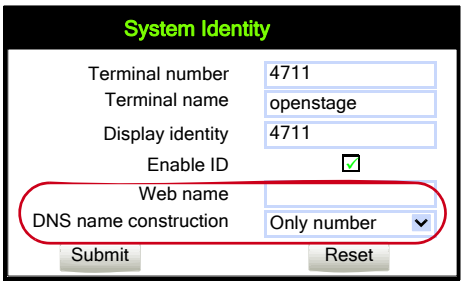
It is recommended to inform the user about the DNS name of his/her phone. The complete WBM address can be found under User menu > Network information > Web address.

The DNS name can be constructed from pre-defined parameters and free text. Its composition is defined by the **DNS name construction** parameter. The following options are available:

- "None":
- "MAC based": The DNS name is built from the prefix "OIP" followed by the phone's MAC address.
- "Web name": The DNS name is set to the the string entered in **Web name**.
- "Only number": The DNS name is set to the **Terminal number**, that is, the phone's call number (see Section 3.5.1, "Terminal and User Identity").
- "Prefix number": The DNS name is constructed from the the string entered in **Web name**, followed by the **Terminal number**.

#### Administration via WBM

System > System Identity




#### Administration via Local Phone

└── Admin
  └── System
    └── Identity
      ├── **Web name**
      └── **DDNS hostname**

## 3.3.8 Configuration & Update Service (DLS)

The Deployment Service (DLS) is a HiPath Management application for administering workpoints in both HiPath and non-HiPath networks. Amongst the most important features are: security (e.g. PSS generation and distribution within an SRTP security domain), mobility for optiPoint and OpenStage SIP phones, software deployment, plug&play support, as well as error and activity logging.

**DLS address**, i.e. the IP address or hostname of the DLS server, and **Default mode port** , i.e. the port on which the DLS server is listening, are required to enable proper communication between phone and DLS.

The **Contact gap** parameter is not used.

Set **Revert to default security** to disable mutual authentication and return to DEFAULT mode. SECURE mode related settings are reset and certificates are removed.

The **Mode** determines whether the communication between the phone and the DLS is secure. A secure connection is established by exchanging credentials between the DLS and the phone for mutual authentication. After this, the communication is encrypted, and a different port is used.

It is possible to operate the DLS server behind a firewall or NAT (Network Address Translation), which prevents the DLS from sending ContactMe messages directly to the phone. Only outbound connections from the phone are allowed. To overcome this restriction, a DLS Contact-Me proxy (DCMP) can be deployed. The phone periodically polls the DCMP (DLS Contact-Me Proxy), which is placed outside of the phone's network, for pending contact requests from the DLS. If there are contact requests, the phone will send a request to the DLS in order to obtain the update, just as with a regular DLS connection.
The URI of the DCMP, as well as the polling interval, are configured by the DLS. For this purpose, it is necessary that the phone establishes a first contact to the DLS, e. g. by phone restart or local configuration change.

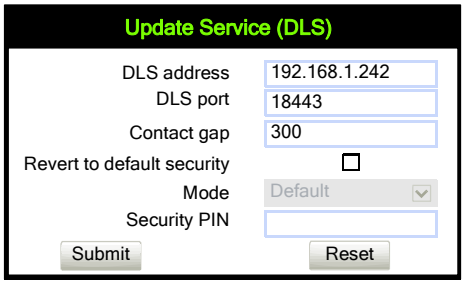
A **Security PIN** can be provided which is used for decrypting data provided by the DLS during bootstrap. For further information, please refer to the DLS documentation.

### Data required

- **DLS address**: IP address or hostname of the server on which the Deployment Service is running.
- **DLS port**: Port on which the DLS Deployment Service is listening.
  Default: 18443
- **Contact gap**: The parameter is not used.
- **Revert to default security**: When set, security mode will be set to default. When using local phone administration, this will be set by selection option '**Default security**' after pressing Save&exit.
- **Mode**: Shows whether the communication between the phone and the DLS is secure.
  Value range: "Default", "Secure", "Secure PIN"
  This parameter is read-only.
- **Security PIN** : Used for enhanced security.

### Administration via WBM

Network > Update Service (DLS)




### Administration via Local Phone

```
└--- Admin
     └--- Network
          └--- Update Service (DLS)
               |--- DLS address
               |--- DLS port
               |--- Contact gap
               |--- Mode
               └--- Security PIN
```

## 3.3.9 SNMP

The Simple Network Management Protocol is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. An SNMP manager surveys and, if needed, configures several SNMP elements, e.g. VoIP phones.

OpenStage phones support SNMPv1.

There are currently 4 trap categories that can be sent by the phones:

### Standard SNMP traps

OpenStage phones support the following types of standard SNMP traps, as defined in RFC 1157:

- **coldStart**: sent if the phone does a full restart.
- **warmStart**: sent if only the phone software is restarted.
- **linkUp**: sent when IP connectivity is restored.

### QoS Related traps

These traps are designed specifically for receipt and interpretation by the QDC collection system. The traps are common to SIP phones, HFA phones, Gateways, etc.

### Traps for important high level SIP related problems

Currently, these traps are related to problems in registering with a SIP Server and to a failure in remotely logging off a mobile user. These traps are aimed at a non-expert user (e.g. a standard Network Management System) to highlight important telephony related problems.

### Traps specific to OpenStage phones

Currently, the following traps are defined:

**TraceEventFatal**: sent if severe trace events occur; aimed at expert users.

**TraceEventError**: sent if severe trace events occur; aimed at expert users.

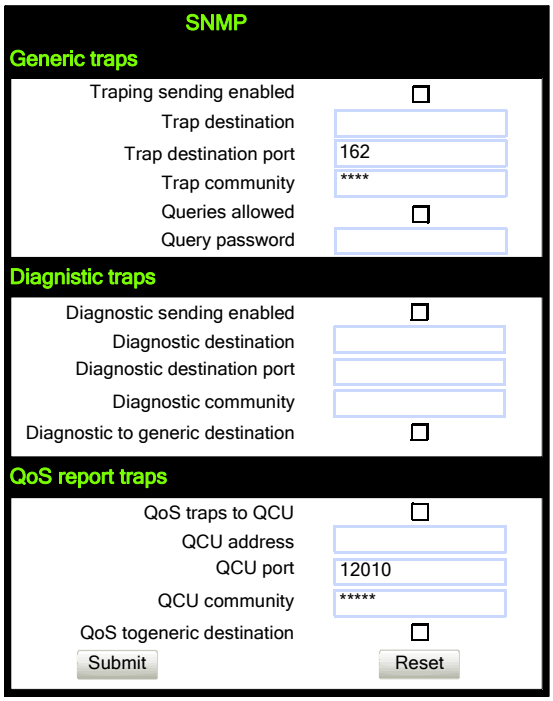
### Data required

- **Trap sending enabled**: Enables or disables the sending of a TRAP message to the SNMP manager.
  Value range: "Yes", "No"
  Default: "No"
- **Trap destination**: IP address or hostname of the SNMP manager that receives traps.
- **Trap destination port**: Port on which the SNMP manager is receiving TRAP messages.
- Default: 162

- **Trap community**: SNMP community string for the SNMP manager receiving TRAP messages.
  Default: "snmp"
- **Queries allowed**: Allows or disallows queries by the SNMP manager.
- **Query password**: Password for the execution of a query by the SNMP manager.
- **Diagnostic sending enabled**: Enables or disables the sending of diagnostic data to the SNMP manager.
  Value range: "Yes", "No"
  Default: "No"
- **Diagnostic destination**: IP address or hostname of the SNMP manager receiving diagnostic data.
- **Diagnostic destination port**: Port on which the SNMP manager is receiving diagnostic data.
- **Diagnostic community**: SNMP community string for the SNMP manager receiving diagnostic data.
- **Diagnostic to generic destination / Diagnostic to generic device**: Enables or disables the sending of diagnostic data to a generic destination.
  Value range: "Yes", "No"
  Default: "No"
- **QoS traps to QCU**: Enables or disables the sending of TRAP messages to the QCU server.
  Value range: "Yes", "No"
  Default: "No"
- **QCU address**: IP address or hostname of the QCU server.
- **QCU port**: Port on which the QCU server is listening for messages.
  Default: 12010.
- **QCU community**: QCU community string.
  Default: "QOSCD".
- **QoS to generic destination**: Enables or disables the sending of QoS traps to a generic destination.
  Value range: "Yes", "No"
  Default: "No"

## Administration via WBM

System > SNMP




## Administration via Local Phone

- Admin
  - System
    - SNMP
      - **Queries allowed**
      - **Query password**
      - **Trap sending enabled**
      - **Trap destination**
      - **Trap destination port**
      - **Trap community**
      - **Diag sending enabled**
      - **Diag destination**
      - **Diag destination port**
      - **Diag community**
      - **QoS traps to QCU**
      - **QCU address**
      - **QCU port**
      - **QCU community**
      - **QoS to generic dest.**

# 3.4 Security

## 3.4.1 Speech Encryption

### 3.4.1.1 General Configuration

OpenStage phones support secure (i.e. encrypted) speech transmission via SRTP. For enabling secure (encrypted) calls, a TLS connection to the Phone Administration server is required.

If **Use secure calls** is activated, the encryption of outgoing calls is enabled, and the phone is capable of receiving encrypted calls. When the phone is connected to an OpenScape Voice system, call security is communicated to the user as follows:

- An icon in the call view tells the user whether a call is secure (encrypted) or not.
- If an active call changes from secure to insecure, e. g. after a transfer, a popup window and an alert tone will notify the user.

For secure (encrypted) calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

In order to use SRTP, the phone must be configured for NTP (for further information please see Section 3.5.5, “Date and Time”). The reason is that the key generation (MIKEY) uses the system time of the particular device as a basis. Thus, encryption will only work correctly if all devices have the same UTC time.

If **SIP server certificate validation** resp. **Backup SIP server certificate validation** is activated, the phone will validate the server certificate sent by the Phone Administration server in order to establish a TLS connection. The server certificate is validated against the root certificate from the trusted certificate authority (CA), which must be stored on the phone first. For delivering the root certificate, a DLS (OpenScape Deployment Service) server is required.

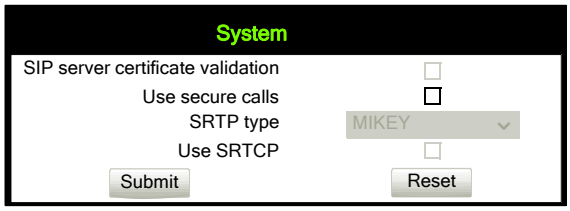
The **SRTP type** sets the key exchange method for SRTP.

When **Use SRTCP** is activated (together with **Use secure calls**), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

If SRTP is enabled, ANAT interworking (see Section 3.5.8.3, “Media/SDP”) is only possible if SDES is configured as the key exchange protocol for SRTP.

### Administration via WBM

System > Security > System




### Administration via Local Phone

```
└── Admin
    └── System
        └── Security
            ├── Server cerfificate
            ├── Use secure calls
            ├── SRTP type
            └── Use SRTCP
```

### 3.4.1.2 MIKEY Configuration

MIKEY (Multimedia Internet KEYing) is a key management protocol that is intended for use with real-time applications. It can specifically be used to set up encryption keys for multimedia sessions that are secured using SRTP.

**Use secure calls** activates the encryption of outgoing calls, i.e. the phone is capable of receiving encrypted calls.

For secure (encrypted) calls, it is required that both endpoints support SRTP. The secure call indication tells the user that the other endpoint has acknowledged the secure connection.

The **SRTP type** sets the key exchange method (negotiation method) for secure calls via SRTP. The following encryption key exchange methods are available:

- MIKEY
- SDES (see Section 3.4.1.3, “SDES Configuration”)

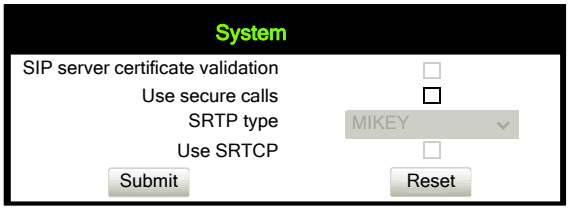
The **SRTP Type** and **Use SRTCP** options are only available for secure (encrypted) calls, i.e. these parameters are only enabled if **Use secure calls** is activated.

When **Use SRTCP** is activated (together with **Use secure calls**), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

If SRTP is enabled, ANAT interworking (see Section 3.5.8.3, “Media/SDP”) is only possible if SDES is configured as the key exchange protocol for SRTP.

### Administration via WBM

System > Security > System




### Administration via Local Phone

- Admin
  - System
    - Security
      - **Server cerfificate**
      - **Use secure calls**
      - **SRTP type**
      - **Use SRTCP**

### 3.4.1.3 SDES Configuration

When "SDES" is selected as SRTP negotiation method (see Section 3.4.1.1, “General Configuration”), it can be configured further.

The **SDES status** parameter enables or disables SDES, just like **SRTP type** in System > Security > System (see Section 3.4.1.1, “General Configuration”). When SDES is disabled, MIKEY will be used.

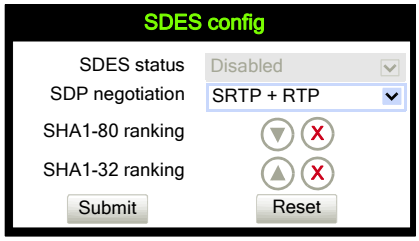
The **SDP negotiation** parameter specifies whether the use of SRTP will be forced by the phone. The following choices are available:

- "RTP + SRTP" - Both non-encrypted (non-secure) and encrypted (secure) media connections are offered. Non-encrypted connections are preferred over encrypted connections, i.e. the phone uses the non-encrypted RTP connection if the remote party accepts it and only switches to SRTP if RTP is not accepted.
- With "SRTP only", only an encrypted (secure) media connection is allowed; if the remote party should not support SRTP, no connection will be established.
- With "SRTP + RTP", the phone will try to establish an SRTP connection, but fall back to RTP if this should fail. This is the recommended option.

With **SHA1-80 ranking** and **SHA1-32 ranking**, the ranking for each crypto-suite for negotiation is defined. Additionally, each crypto-suite can be enabled or disabled.

#### Administration via WBM

System > Security > SDES config



## 3.4.2 Access Control

The **CCE access** parameter controls TCP access for the CCE (CommsChannel Extender). This affects the operation of the OpenStage Manager, local CTI access, and HPT access. When "Disable" is selected, TCP is disabled. With "Enable", there are no restrictions.

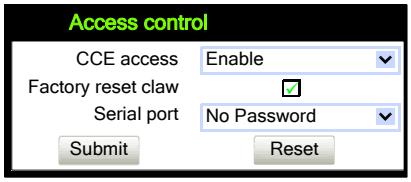
With **Factory reset claw**, the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access can be enabled or disabled.

The **Serial port** parameter controls access to the serial port. When set to "No password", a terminal connected to the port can interact with the phone's operating system without restrictions. When "Passwd reqd" is selected, the serial port requires a password for access (root user is not available). When "Unavailable" is chosen, the serial port is not accessible.

As a prerequisite, the root user needs to create a user and to define a password via Serial Access, so that access can be granted when the **Password required** prompt is issued.

### Administration via WBM

System > Security > Access control



## 3.4.3 Security Log

A circular security log is used to capture important security specific events. It can be exported as CSV data to an external application for analysis.

The security log cannot be disabled.

The **Max. lines** parameter defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten by new entries.

**Archive to DLS** controls whether the log is sent to the DLS. When activated, the DLS is used to automatically archive the security log so that no log entries will be lost.

With **Archive when at**, the trigger for log archiving is set. Automatic archiving of new security log entries will occur when the percentage of unarchived entries in the log is as specified or more. When set to disabled, every new entry will trigger a save (only possible via DLS). The possible values are "10%", "20%", "30%", "35%", "40%", "45%", "50%", "55%", "60%", "65%", "70%", "80%", "90%".

The security log upload may be accomplished in two ways:

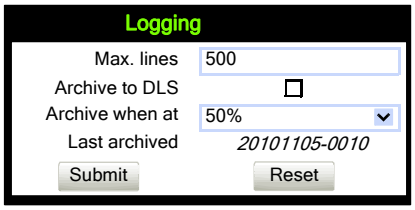
- If "Archive to DLS" is enabled, if the security log reaches the threshold % for unachieved entries, the phone will initiate an upload.
- If "Archive to DLS" is NOT enabled and the security log reaches the threshold % for unachieved entries, the phone only sets the "archive-me" flag, it does not initiate the archive.

It is up to the DLS to recognize the flag and initiate an upload.

**Last archived** shows the date when the security log was last archived to the DLS.

### Administration via WBM

System > Security > Logging



### 3.4.4 Security-Related Faults

**Security log entry** shows the date and time of a loss of security log entries.

> The entries in this list are only displayed until they are reported to the DLS, which usually happens very fast. After that, the entries are automatically deleted from the phone. If the entries are not deleted automatically, they can be deleted manually by using the "Cancel faults" parameter.

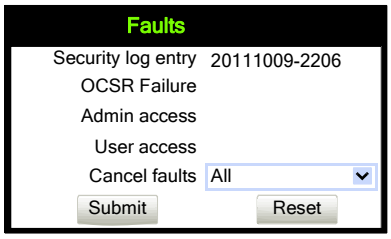
**OCSR failure** shows the date and time when the phone was unable to connect to any certificate checking server for revoked certificates.

**Admin access** shows the date and time when the phone encountered multiple consecutive failures to enter the admin password.

**User access** shows the date and time when the phone encountered multiple consecutive failures to enter the user password.

#### Administration via WBM

System > Security > Faults



## 3.4.5 Password Policy

### 3.4.5.1 General Policy

**Expires after (days)** sets the maximum validity period of a password.

**Warn before (days)** specifies when the user/admin is notified that his password will expire.

**Force changed** only affects the User password. When **Force changed** is activated, the user will be forced to change his/her password at next login. This only applies to users, not to administrators.

**Tries allowed** specifies the maximum number of password entry trials before the password is suspended. Values: 0 (no limits), 2, 3, 4, 5

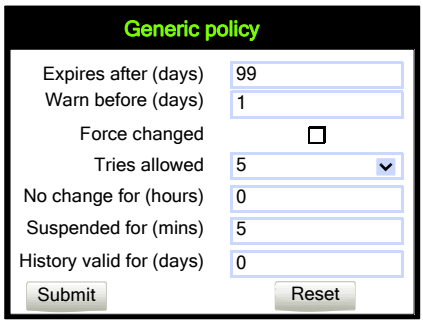
**No change for (hours)** specifies a period before a password is allowed to be changed again. Value range: 0 to 99

**Suspended for (mins)** defines how long a password will be suspended after the number of failed retries has exceeded. Value range: 0 to 99

**History valid for (days)** defines a period in days during which the history is valid. Passwords no longer used are kept in history lists for the user and admin passwords to prevent reuse of past passwords. This list is organised as FIFO (First In, First Out) so that it always contains the latest passwords.

**Administration via WBM**

Security and Policies > Password > Generic Policy



### 3.4.5.2 Admin Policy

**Expiry date** shows the date and time when the admin password will expire.

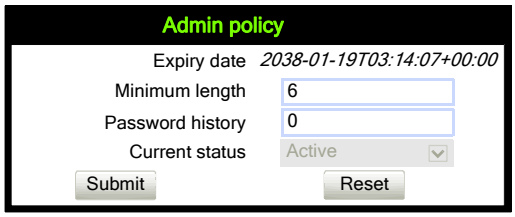
**Minimum length** defines the minimum number of characters for the admin password.

**Password history** specifies the number of entries to be kept in the admin password history. New passwords must not match any password in the history.

The **Current status** parameter determines the status for the admin password. When set to "Active", the admin password is available for use. With "Suspended", the admin password is not available for a period or until reset. When set to "Disabled", all access via the admin password is disabled. The status of the admin password can only be set via DLS/WPI. It is changed internally to "suspended" when the password has been entered incorrectly more times than allowed.

#### Administration via WBM

Security and Policies > Password > Admin Policy



### 3.4.5.3 User Policy

**Expiry date** shows the date and time when the user password will expire.

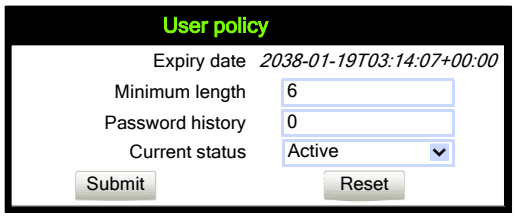
**Minimum length** defines the minimum number of characters for the user password.

**Password history** specifies the number of entries to be kept in the user password history.

The **Current status** parameter determines the status for the user password. When set to "Active", the user password is available for use. With "Suspended", the user password is not available for a period or until reset. When set to "Disabled", all access via the user password is disabled.

**Administration via WBM**

Security and Policies > Password > User Policy




### 3.4.5.4 Character Set

The composition of the password can be configured in detail.

**Ucase chars reqd.** defines the minimum number of uppercase characters. Value range: 0 to 24

**Lcase chars reqd.** defines the minimum number of lowercase characters. Value range: 0 to 24

**Digits required** defines the minimum number of digits. 0 to 24

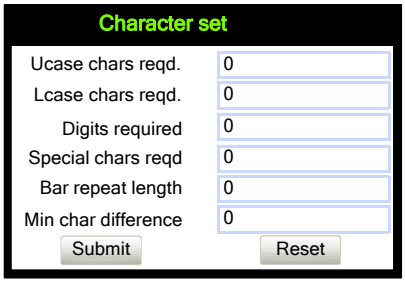
**Special chars reqd** defines the minimum number of special characters. The set of possible characters is ` - = [ ] ; ’ # \ , . / ¬ ! ” £ $ % ^ & * ( ) _ + { } : @ ~ | < > ?
Value range: 0 to 24

**Bar repeat length** specifies the maximum number of consecutive uses of a character. Value range: 0 to 24, but not 1 (with 1 set as value, no password would be valid, because it would be forbidden to use any character once).

**Min char difference** specifies the minimum number of characters by which a new password must differ from the previous password. Value range: 0 to 24

### Administration via WBM

Security and Policies > Password > Character set

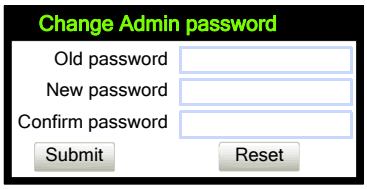



## 3.4.5.5 Change Admin and User password

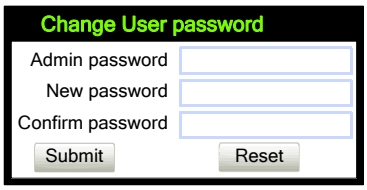
The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting for the Admin password is "123456"; it should be changed after the first login (Password handling in previous versions see Section 3.20, “Password”).

### Administration via WBM

Security and Policies > Password > Change Admin password




Security and Policies > Password > Change User password




### Administration via Local Phone

- Admin
  - Security & policies
    - Password
      - Change **Admin** password
        - Current password
        - New password
        - Confirm password
      - Change **User** password
        - Admin password
        - New password
        - Confirm password

## 3.4.6 Certificate Policy

### 3.4.6.1 Online Certificate Check

The Online Certificate Status Protocol (OCSP) is used to check if a certificate to be used has been revoked. This protocol is used to query an Online Certificate Status Responder (OCSR) at the point when the certificate is being validated. The address of an OCSR can be configured on the phone and can also be obtained from the certificate to be checked (which will have the priority).

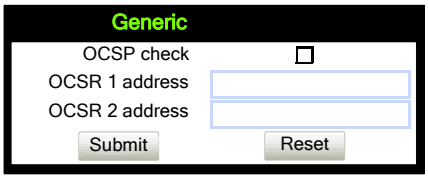
When **OCSP check** is activated, the configured OCSR is requested to check if the certificate has been revoked.

**OCSR 1 address** specifies the IP address (or FQDN) of a primary OCSP responder.

**OCSR 2 address** specifies the IP address (or FQDN) of a secondary OCSP responder.

**Administration via WBM**

Security and Policies > Certificates > Generic



### 3.4.6.2 Server Authentication Policy

For individual certificates provided by specific servers, the level of authentication can be configured. When "None" is selected, no certificate check is performed. With "Trusted", the certificate is only checked against the signature credentials provided by the remote entity for signature, and the expiry date is checked. When "Full" is selected, the certificate is fully checked against the credentials provided by the remote entity for signature, the fields must match the requested subject/usage, and the expiry date is checked.

**Secure file transfer** sets the authentication level for the HTTPS server to be used (see Section 3.16.2, “Common FTP/HTTPS Settings”).

**Secure send URL** sets the authentication level for the server to which special HTTP requests are sent on key press ("Send URL" function, see Section 3.8.30, “Send Request via HTTP/HTTPS”).

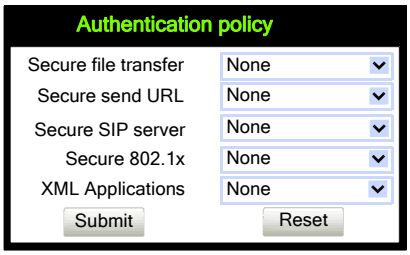
**Secure SIP server** sets the authentication level for the SIP server connected to the phone (see Section 3.5.7, “SIP Registration”).

**Secure 802.1x** sets the authentication level for the 802.1x authentication server.

**XML Applications** sets the authentication level for the XML applications server (see Section 3.19, “Applications”).

#### Administration via WBM

Security and Policies > Certificates > Authentication policy




#### Administration via Local Phone

```
└── Admin
    └── Security & policies
        └── Certificates
            └── Authentication policy
                ├── Secure file transfer
                └── Secure send URL
```

# 3.5 System Settings

## 3.5.1 Terminal and User Identity

### 3.5.1.1 Terminal Identity

Within a SIP environment, both Terminal Number and Terminal Name may serve as a phone number. The values are used in the userinfo part of SIP URIs.

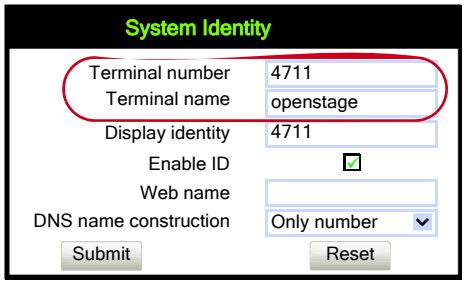
In order to register with a SIP registrar, the phone sends REGISTER messages to the registrar containing the contents of **Terminal number**.

#### Data required

- **Terminal number**: Number to be registered at the SIP registrar.
- **Terminal name**: Name to be registered at the SIP registrar.

#### Administration via WBM

System > System Identity




#### Administration via Local Phone

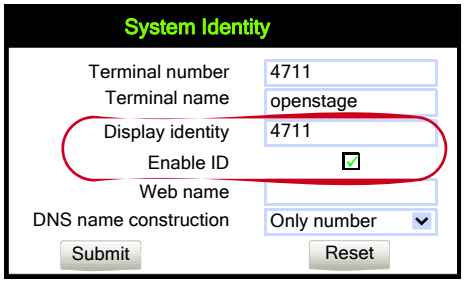
```
└--- Admin
    └--- System
        └--- Identity
            |--- Terminal number
            └--- Terminal name
```

### 3.5.1.2 Display Identity

If an individual name or number is entered as **Display identity** and **Enable ID** is activated, it is displayed in the phone's status bar instead of the Terminal number.

## Administration via WBM

System > System Identity




## Administration via Local Phone

```
└── Admin
    └── System
        └── Identity
            ├── Display identity
            └── Enable ID
```

## 3.5.2 Emergency and Voice Mail

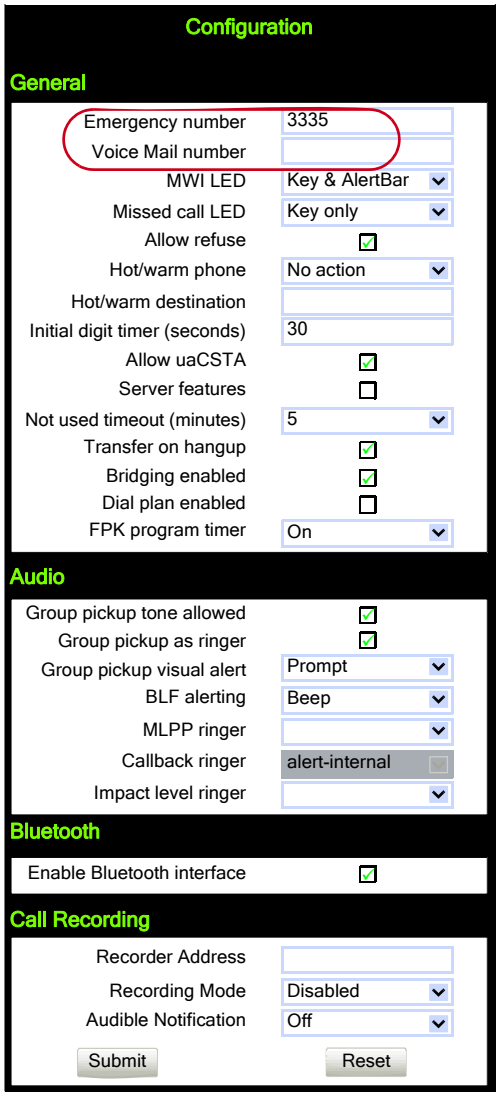
It is important to have an **Emergency number** configured. If the phone is locked, a clickable area for making an emergency call is created.

> If more than one emergency number is needed, additional numbers can be configured in the canonical dial settings (Section 3.13.1, “Canonical Dialing Configuration”).

If a mailbox located at a remote server shall be used, its **Voice mail number** must be entered.

### Administration via WBM

System > Features > Configuration



### Administration via Local Phone

```
└--- Admin
     └--- System
          └--- Features
               └--- Configuration
                    └--- General
                         ├--- Emergency number
                         └--- Voicemail number
```

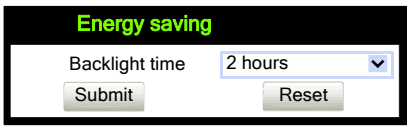
## 3.5.3 Energy Saving (OpenStage 40/60/80)

After the phone has been inactive within the timespan specified in **Backlight time**, the display backlight is switched off to save energy.

The possible values are: 1 minute, 5 minutes, 30 minutes, 60 minutes, 2 hours, 4 hours or 8 hours. Moreover, with OpenStage 40 and 60, this parameter can also be configured by the user.

### Administration via WBM

Local functions > Energy saving




### Administration via Local Phone

```
└--- Admin
     └--- Local Functions
          └--- Energy saving
               └--- Backlight time
```

## 3.5.4 Call logging

This configuration item allows the phone to detect if a number dialled by the User is likely to be a Feature Access Code (FAC) by comparing the start of the dialled number with the configured FAC prefixes. If the dialled number does match a FAC prefix and the SIP server has provided a different number for the called party then the number shown in the Dialled tab list of Call Log is changed from the dialled number to the server provided number. If the new configuration item is left empty then the Dialled tab list display will remain as currently populated (i.e. the dialled number is shown in the list).

A further enhancement for an entry matched to a FAC in the Dialled tab list of Call Log is that the context menu for the list entry now provides both numbers from the last call associated with the entry as Dial options in the context menu for the list entry (similar to that already provided by the context menu for the Details form of such an entry). Note that the Call Log display on OS15 has been simplified [3] so that an entry only displays a name or a number (not both) and there is no access to entry details. However this only limits the display and the default dialling number for an OS15 entry is determined as above.

Call Log entry grouping rules for the Dialled tab list remain unchanged, if multiple FACs all map to numbers associated with one contact then they are grouped together.

### Data required

- **FAC prefixes**: A comma separated list of feature prefixes considered to represent feature codes configured at the SIP server for abbreviated dialling.

### Administration via WBM

Local functions > Call logging

### 3.5.4.1 Logging of Missed Calls (via User menu)

This feature allows the user to

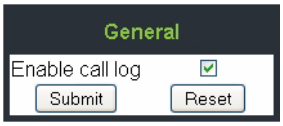
- distinguish logged calls based on the device on which the calls were completed, and
- decide whether missed calls that were answered elsewhere shall be
  - included into the call log, or
  - excluded from the call log, i.e. not logged at all
- decide whether a number which also exists in missed calls tab of call log is to be deleted from call log when this number is called
  - manually
  - when called

In the **Call Lists**, missed calls that were completed elsewhere are marked with a check mark. For details, please refer to the *User manual*.

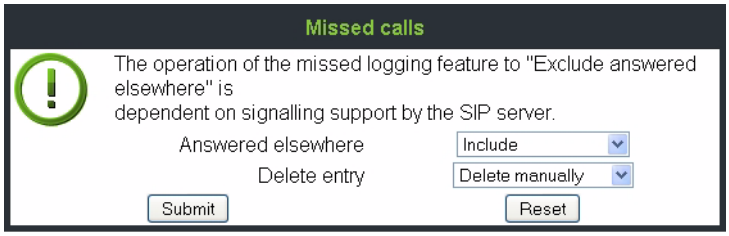
Forwarded calls are not logged under "Missed calls", but under "Forwarded" in the call log.

**Administration via WBM (User menu)**

User > Configuration > Call logging > General




User > Configuration > Call logging > Missed calls



### Administration via Local Phone (User menu)

- User
  - Configuration
    - **Call logging**
      - **General**
        - **FAC prefixes**
      - **Missed calls**
        - **Answered elsewhere**
          - **Include**
          - **Exclude**
        - **Delete entry**
          - **Manually**
          - **When called**

**Answered elsewhere > Include**: Calls completed elsewhere will be logged as missed calls. In the call log these calls are marked with a check mark.

**Answered elsewhere > Exclude**: Calls completed elsewhere will not be visible on phone; they will not be logged at all.

**Delete entry > Manually** : Call numbers remain in call log until they are deleted manually.

**Delete entry > When called**: Call numbers existing in missed call list are deleted automatically when they are called again.

## 3.5.5 Date and Time

If the DHCP server in your network provides the IP address of the SNTP server, no manual configuration is necessary. If not, you have to set the **SNTP IP address** parameter manually.

For correct display of the current time, the **Timezone offset** must be set appropriately. This is the time offset from UTC (Universal Time Coordinated). If, for instance, the phone is located in Munich, Germany, the offset is +1 (or simply 1); if it is located in Los Angeles, USA, the offset is -8. For countries or areas with half-our time zones, like South Australia or India, non-integer values can be used, for example 10.5 for South Australia (UTC +10:30).

If the phone is located in a country with DST (Daylight Saving Time), you can choose whether DST is toggled manually or automatically. For manual toggling, disable **Auto time change** and enable or disable **Daylight saving**; the change will be in effect immediately. For automatical toggling, enable **Auto time change**; now, daylight saving is controlled by the **DST zone / Time zone** parameter. This parameter determines when DST starts or ends, and must be set according to the location of the phone.

The **Difference (minutes)** parameter defines how many minutes the clock is put forward for DST. In Germany, for instance, the value is +60.

Please note that **Difference (minutes)** must be specified both for manual and automatic DST toggling.

### 3.5.5.1 SNTP is Available, but no Automatic Configuration by DHCP server

**Data required**

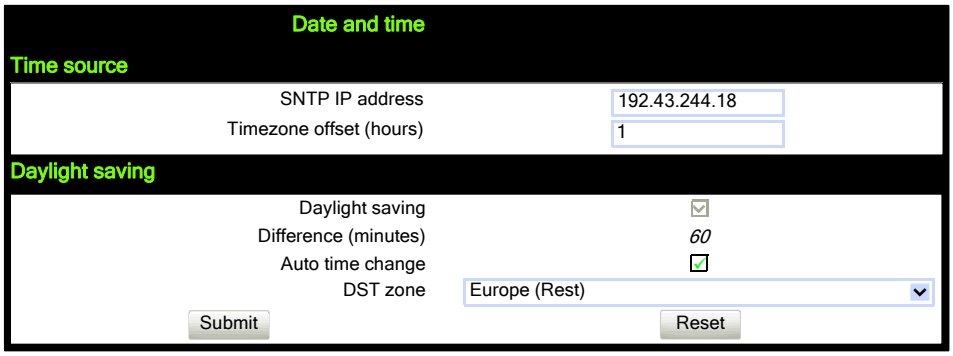
- **SNTP IP address**: IP address or hostname of the SNTP server.
- **Timezone offset (hours)**: Shift in hours corresponding to UTC.
- **Daylight saving**: Enables or disables daylight saving time in conjunction with **Auto time change**.
  Value range: "Yes", "No"
  Default setting for **OpenStage 40 US** is "**Yes**". After a factory reset, the system will be reset to this value.
- **Difference (minutes)**: Time difference when daylight saving time is in effect.
  Default setting for **OpenStage 40 US** is "**60 (mins)**". After a factory reset, the system will be reset to this value.
- **Auto time change** / **Auto DST**: Enables or disables automatic control of daylight saving time according to the **Time zone**.
  Value range: "Yes", "No"
  Default setting for **OpenStage 40 US** is "**Yes**". After a factory reset, the system will be reset to this value.

- **Time zone** / **DST zone**: Area with common start and end date for daylight saving time. Value range: "Australia 2007 (ACT, South Australia, Tasmania, Victoria)", "Australia 2007 (New South Wales)", "Australia (Western Australia)", "Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria)", "Brazil", "Canada", "Canada (Newfoundland)", "Europe (Portugal, United Kingdom)", "Europe (Finland)", "Europe (Rest)", "Mexico", "United States", "New Zealand", "New Zealand (Chatham)".

  Default setting for **OpenStage 40 US** is "**United States**". After a factory reset, the system will be reset to this value.

### Administration via WBM

Date and Time




### Administration via Local Phone

```
└--- Admin
    └--- Date and Time
        ├--- SNTP IP address
        └--- Timezone offset
```

### 3.5.5.2 No SNTP Server Available

If no SNTP server is available, date and time must be set manually.

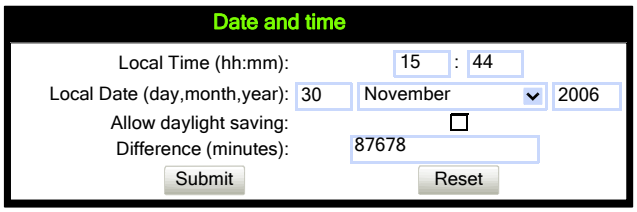
The manual setting of time and date is located in the user menu, not in the administrator menu.

#### Data required

- **Local time (hh:mm)**: Local time.
- **Local date (day, month, year)**: Local date.
- **Allow daylight saving**: Defines whether there is daylight is set.
- **Difference (minutes)**: Timezone offset in minutes.
- **Auto time change** / **Auto DST**: Enables or disables automatic control of daylight saving time according to the **Time zone**.
  Value range: "Yes", "No"
  Default setting for **OpenStage 40 US** is "**Yes**". After a factory reset, the system will be reset to this value.

#### Administration via WBM (User menu)

User > Date and time




#### Administration via Local Phone

└── Menu
  └── Date and Time
    ├── **Time**
    ├── **Date**
    ├── **Daylight saving**
    ├── **Difference (mins)**
    └── **Auto DST**

## 3.5.6 SIP Addresses and Ports

### 3.5.6.1 SIP Addresses

In this group of parameters, the IP addresses or host names for the SIP server, the SIP registrar, and the SIP gateway are defined.

**SIP server address** provides the IP address or host name of the SIP proxy server (OpenScape Voice). This is necessary for outgoing calls. **SIP registrar address** contains the IP address or host name of the registration server, to which the phone will send REGISTER messages. When registered, the phone is ready to receive incoming calls. **SIP gateway address** gives the IP address or host name of the SIP gateway. If configured, the SIP gateway is used for outgoing calls; otherwise the server specified in **SIP server address** is used. A SIP gateway is able to perform a conversion of SIP to TDM, which enables to send calls directly into the public network.

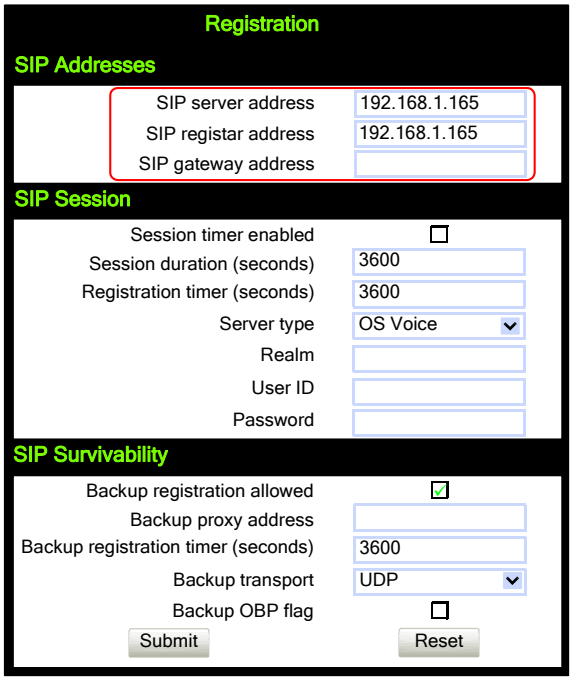
Enhanced survivability using DNS SRV is available. To make use of it, a special configuration is required. For details, please refer to Section 3.5.10, “Resilience and Survivability”.

**Data required**

- **SIP server address**: IP address or host name of the SIP proxy server.
- **SIP registrar address**: IP address or host name of the registration server.
- **SIP gateway address**: IP address or host name of the SIP gateway.

## Administration via WBM

System > Registration




## Administration via Local Phone

- Admin
  - System
    - Registration
      - SIP Addresses
        - **SIP server**
        - **SIP registrar**
        - **SIP gateway**

### 3.5.6.2 SIP Ports

In this group of parameters, the ports for the SIP server, the SIP registrar, and the SIP gateway are defined (for further information see Section 3.5.6.1, “SIP Addresses”), as well as the SIP port used by the phone (**SIP local**).

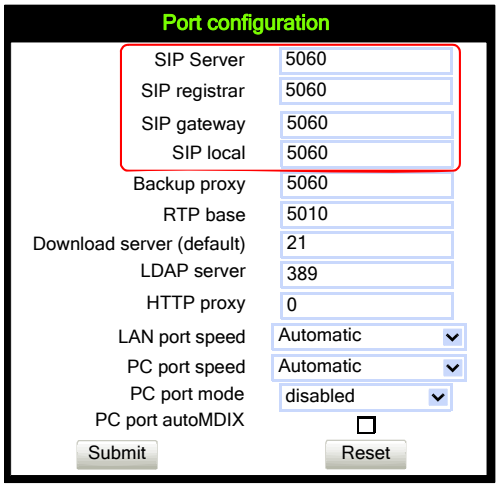
#### Data required

- **SIP server**: Port of the SIP proxy server.
  Default: 5060.
- **SIP registrar**: Port of the server at which the phone registers.
  Default: 5060.
- **SIP gateway**: Port of the SIP gateway.
  Default: 5060.
- **SIP local**: Port used by the phone for sending and receiving SIP messages.
  Default: 5060.

When changing the SIP Transport protocol from UDP/TCP to TLS, the SIP port now also have to be changed correspondingly (e.g. SIP port from 5060 to 5061) and on changing vice versa.

#### Administration via WBM

Network > Port configuration




#### Administration via Local Phone

└── Admin
  └── Network

└--- Port Configuration
  ├--- **SIP server**
  ├--- **SIP registrar**
  ├--- **SIP gateway**
  └--- **SIP local**

## 3.5.7 SIP Registration

Registration is the process by which centralized SIP Server/Registrars become aware of the existence and readiness of an endpoint to make and receive calls. The phone supports a number of configuration parameters to allow this to happen. Registration can be authenticated or un-authenticated depending on how the server and phone is configured.

For operation with an OpenScape Voice server, set **Server type** to "OS Voice". When HiQ8000 is to be used, set it to "HiQ8000". The expiry time of a registration can be specified by **Registration timer**.

### Unauthenticated Registration

For unauthenticated registration, the following parameters must be set on the phone: Terminal number or Terminal name (see Section 3.5.1.1, “Terminal Identity”), SIP server and SIP registrar address (see Section 3.5.6.1, “SIP Addresses”).

In unauthenticated mode, the server must pre-authenticate the user. This procedure is server specific and is not described here.

### Authenticated Registration

The phone supports the digest authentication scheme and requires some parameters to be configured in addition to those for unauthenticated registration. By providing a **User ID** and a **Password** which match with a corresponding account on the SIP registrar, the phone authenticates itself. Optionally, a **Realm** can be added. This parameter specifies the protection domain wherein the SIP authentication is meaningful. The protection domain is globally unique, so that each protection domain has its own arbitrary usernames and passwords.

A challenge from the server for authentication information is not only restricted to the REGISTER message, but can also occur in response to other SIP messages, e. g. INVITE.

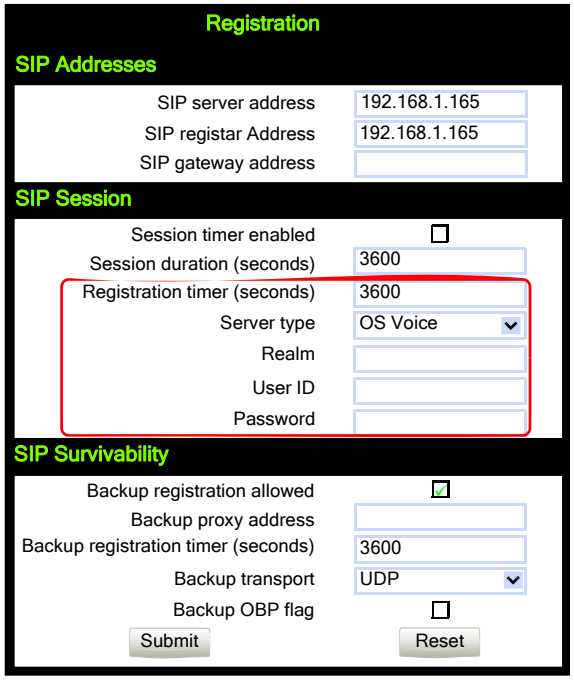
If registration has not succeeded at startup or registration fails after having been previously successfully registered the phone will try to re-register every 30 seconds. This is not configurable.
If the registration is not answered at all, the phone will try to re-register every 60 seconds by default. This is configurable (see Maximum Registration Backoff Timer → page 120).

## Data required

- **Registration timer (seconds)**: Expiry time of the registration in seconds.
  Default value: 3600.
- **Server type**: Type of server the phone will register to.
  Value range: "Other", "OS Voice", "HiQ8000", "Genesys"
  Default value: "OS Voice"
- **Realm**: Protection domain for authentication.
- **User ID**: Username required for an authenticated registration.
- **Password**: Password required for an authenticated registration.

## Administration via WBM

System > Registration




## Administration via Local Phone

```
└── Admin
    └── System
        └── Registration
            └── SIP Session
                ├── Registration timer
                ├── Server type
                ├── Realm
                ├── User ID
                └── Password
```

## 3.5.8 SIP Communication

### 3.5.8.1 Outbound Proxy

If this option is set to "Yes", the phone routes outbond requests to the configured proxy. The outbound proxy will fulfill the task of resolving the domain contained in the SIP request. If "No" is set, the phone will attempt to resolve the domain by itself.

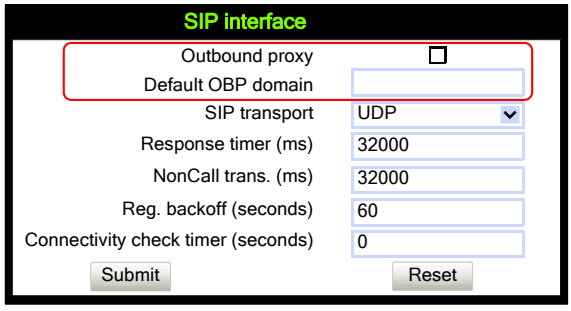
If a **Default OBP** (Outbound Proxy) **domain** is set and the number or name dialed by the user does not provide a domain, this value will be appended to the name or number. Otherwise, the domain of the outbound proxy will be appended.

#### Data required

- **Outbound proxy**: Determines whether an outbound proxy is used or not.
  Value range: "Yes", "No"
  Default: "Yes"; when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "Yes"
- **Default OBP domain**: Alternative value for the domain that is given in the outbound request.

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

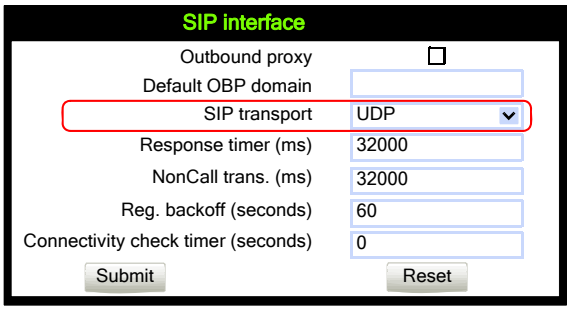
```
└── Admin
    └── System
        └── SIP Interface
            ├── Outbound proxy
            └── Default OBP domain
```

### 3.5.8.2 SIP Transport Protocol

Selects the transport protocol to be used for SIP messages. The values "UDP", "TCP", and "TLS" are available. The default is "UDP"; default when System > Registration > Server type is set to "HiQ8000" (firmware version V3 onwards): "TLS".

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

└--- Admin
  └--- System
    └--- SIP Interface
      └--- **SIP transport**

### 3.5.8.3 Media/SDP

OpenStage phones support IPv4/IPv6 media address negotiation in SDP using ANAT (Alternative Network Address Types). ANAT allows for for the expression of alternative network addresses (e. g., different IP versions) for a particular media stream.

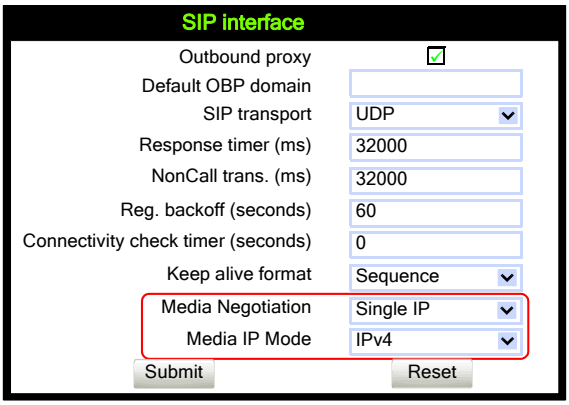
When **Media negotation** is set to "ANAT", ANAT is supported; the phone will re-register with the SIP server and advertise ANAT support in the SIP header. When set to "Single IP", ANAT support is disabled.

If SRTP is enabled, ANAT interworking is only possible if SDES is configured as the key exchange protocol for SRTP (see Section 3.4.1.1, “General Configuration”).

**Media IP mode** defines which IP version is to be used for voice transmission. With "IPv4", only IPv4 is used; with "IPv6", only IPv6 is used; with "IPv4_IPv6", both IPv4 and IPv6 can be used, but IPv4 is preferred; with "IPv6_IPv4", both IPv6 and IPv4 can be used, but IPv6 is preferred.

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

Admin
System
SIP Interface
**Media negotiation**
**Media IP mode**

## 3.5.9 SIP Session Timer

Session timers provide a basic keep-alive mechanism between 2 user agents or phones. This mechanism can be useful to the endpoints concerned or for stateful proxies to determine that a session is still alive. This is achieved by the phone sending periodic re-INVITEs to keep the session alive. If no re-INVITE is received before the interval passes, the session is considered terminated. Both phones are supposed to terminate the call, and stateful proxies can remove any state for the call.

This feature is sufficiently backward compatible such that only one end of a call needs to implement the SIP extension for it to work.

The parameter **Session timer enabled** determines whether the mechanism shall be used, and **Session duration (seconds)** sets the expiration time, and thus the interval between refresh re-INVITEs.

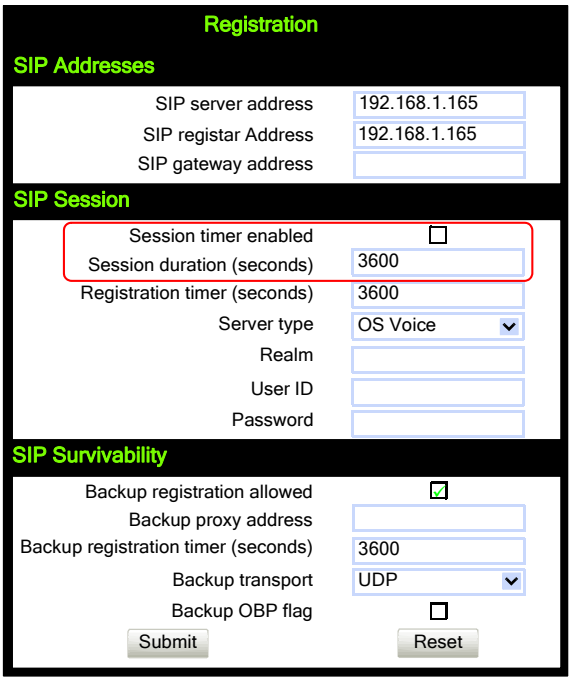
Some server environments support their own mechanism for auditing the health of a session. In these cases, the **Session timer** must be deactivated.
For OpenScape Voice, the **Session timer** should be deactivated.

**Data required**

- **Session timer enabled**: Activates or deactivates the session timer mechanism.
  Value range: "Yes", "No"
  Default value: "No"
- **Session duration (seconds)**: Sets the expiration time for a SIP session.
  Default: 3600

## Administration via WBM

System > Registration




## Administration via Local Phone

```
└── Admin
    └── System
        └── Registration
            └── SIP session
                ├── Session timer
                └── Session duration
```

## 3.5.10 Resilience and Survivability

To allow for stable operation even in case of network or server failure, OpenStage phones have the capability of switching to a fallback system. The switchover is controlled by various configurable check and timeout intervals.

Survivability is achieved in two different ways:

1. DNS SRV can be used for enhanced survivability, either in a scenario with a survivability proxy, or in a scenario with multiple primary SIP servers. The DNS server provides the phone with a prioritized list of SIP servers via DNS SRV. The phone fetches this list periodically from the server, depending on the TTL (time to live) specified for the DNS SRV records.

   To enable DNS SRV requests from the phone, please make the following settings:

   - Specifiy the IP address of the DNS server that provides the server list via DNS SRV. The web interface path is Network > IP configuration > Primary DNS. For details, see Section 3.3.7.2, “DNS Servers”.
   - Enable the use of an outbound proxy for routing outbound requests. The web interface path is System > SIP interface > Outbound proxy. For details, see Section 3.5.8.1, “Outbound Proxy”.
   - Set the SIP gateway port to 0. The web interface path is Network > Port configuration > SIP gateway. Alternatively, if the SIP server otherwise specified in System > Registration > SIP server address is to be configured by DNS SRV, set the SIP server port to 0. The web interface path is Network > Port configuration > SIP server. For details, see Section 3.5.6.2, “SIP Ports”.
   - As SIP gateway address, enter the DNS domain name for which the DNS SRV records are valid. The web interface path is System > Registration > SIP gateway address. Alternatively, if the SIP server otherwise specified in System > Registration > SIP server address is to be configured by DNS SRV, set the mentioned parmeter to the DNS domain name for which the DNS SRV records are valid. For details, see Section 3.5.6.1, “SIP Addresses”.

   A survivability proxy acts as a relay between the phone and the primary SIP server. Thus, the address of the survivability proxy is specified as gateway or SIP server at the phone (see Section 3.5.7, “SIP Registration”). When the TLS connection between the survivability proxy and the SIP server breaks down, e. g. because of server failure, the survivable proxy itself acts as a replacement for the primary SIP server. Vice versa, in case the phone can not reach the survivability proxy itself, it will register directly with the primary SIP server, provided that it is specified in the DNS SRV server list.

   The survivability proxy notifies the phone whenever the survivability changes, so it can indicate possible feature limitations to the user. Furthermore, to enhance survivability, the phone will be kept up-to-date about the current survivability state even after a restart.

Another way to realize survivability is the use of multiple, geographically separated SIP servers. Normally, the phone is registered with that server that has the highest priority in the DNS SRV server list. If the highest priority server fails to respond to the TLS connectivity check (see Section 3.5.10.1, “TLS Connectivity Check”), the phone will register with the server that has the second highest priority.

2. Use of a Backup SIP Server. Along with the registration at the primary SIP server, the phone is registered with a backup SIP server. In normal operation, the phone uses the primary server for outgoing calls. If the phone detects that the connection to the primary SIP server is lost, it uses the backup server for outgoing calls. This connection check is realized by 2 timers; for details, see Section 3.5.10.2, “Response Timer” and Section 3.5.10.3, “Non-INVITE Transaction Timer”. For configuring the backup server, please refer to Section 3.5.10.5, “Backup SIP Server”.

In survivability mode, some features will presumably not be available. The user will be informed by a message in the Call View display.

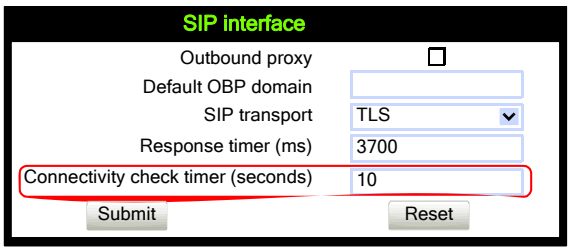
### 3.5.10.1 TLS Connectivity Check

A regular check ensures that the TLS link to the main SIP server is active. When the **Connectivity check timer** is set to a non-zero value, test messages will be sent at the defined interval. If the link is found to be dead, the phone uses DNS SRV to find another SIP server. Certainly, the DNS SRV records must be properly configured in the DNS server.

If no other primary SIP server is found via DNS SRV, the phone will switch over to a backup server for making receiving calls. For configuring the backup server, please refer to Section 3.5.10.5, “Backup SIP Server”.

#### Administration via WBM

System > SIP interface



### 3.5.10.2 Response Timer

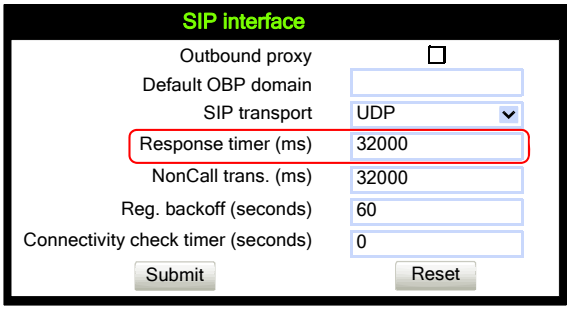
The **Response Timer** resp. **Call trans** timer is started whenever the phone sends a new INVITE message to the SIP server.

If the call transaction timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If there is no backup server configured, the phone just tidies up internally.

The data is given in milliseconds. The default value is 32 000; for Phone Administration, the recommended setting is 3.7 seconds (3700 ms).

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

Admin
System
SIP Interface
**Call trans. (ms)**

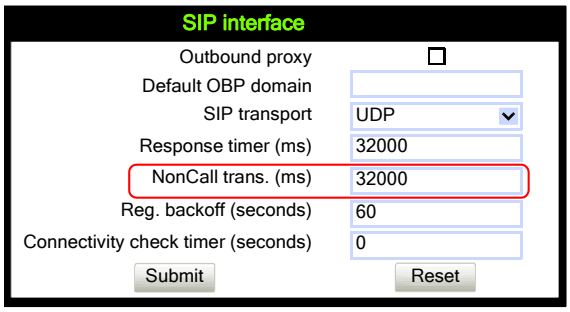
### 3.5.10.3 Non-INVITE Transaction Timer

The **NonCall trans** timer is started whenever the phone sends a non-INVITE message to the SIP server. If the timer expires before the phone gets a response from the SIP server, the phone assumes that the server had died and then attempts to contact the backup server, if configured. If no backup server is configured, the phone will just tidy up internally.

The data is given in milliseconds. The default value is 32 000; for Phone Administration, the recommended setting is 6 seconds (6000 ms).

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

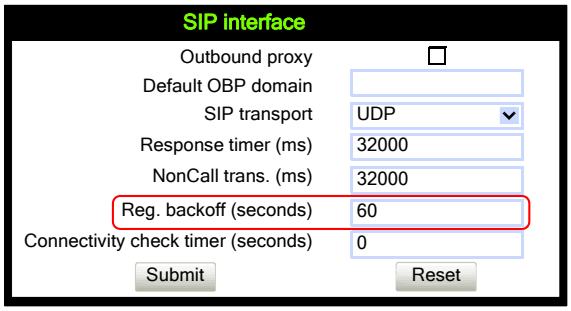
└── Admin
  └── System
    └── SIP Interface
      └── **NonCall transactions (ms)**

### 3.5.10.4 Maximum Registration Backoff Timer

If a registration attempt should result in a timeout, the phone waits a random time before sending another REGISTER message. The **Reg. backoff (seconds)** parameter determines the maximum waiting time.

#### Administration via WBM

System > SIP interface




#### Administration via Local Phone

└── Admin
    └── System
        └── SIP Interface
            └── **Reg. backoff**

### 3.5.10.5 Backup SIP Server

The **Backup registration flag** indicates whether or not the phone treats the backup proxy server as a SIP registrar. If set to "Yes", the phone tries to register its SIP address with the server whose IP address or hostname is specified by **Backup proxy address**. Once an IP address has been entered, the SIP-UDP Port is opened, even if SIP-TLS is used for the OS Voice connection.

The **Backup registration timer** determines the duration of a registration with the backup SIP server.

The **Backup transport** option displays the current transport protocol used to carry SIP messages to the Backup proxy server.

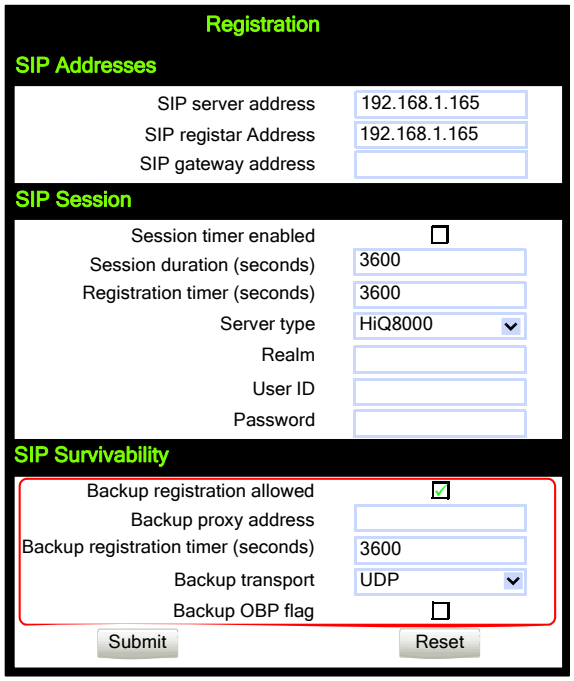
The **Backup OBP flag** indicates whether or not the Backup proxy server is used as an outbound proxy.

**Data required**

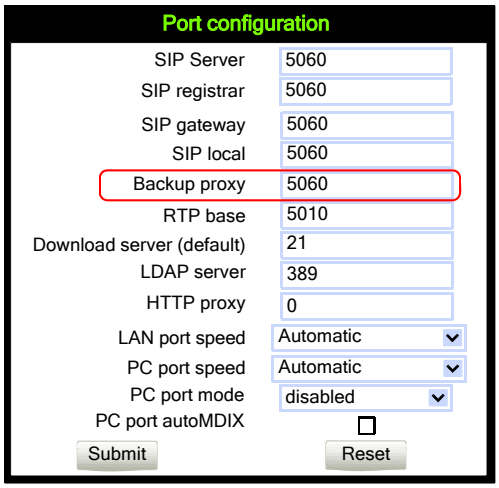
- **Backup registration allowed / Backup registration flag**: Determines whether or not the backup proxy is used as a SIP Registrar.
  Value Range: "Yes", "No"
  Default: "Yes"
- **Backup proxy address**: IP address or hostname of the backup proxy server.
- **Backup registration timer**: Expiry time of the registration in seconds.
  Default: 3600
- **Backup transport**: Transport protocol to be used for messages to the backup proxy.
  Value range: "TCP", "UDP"
  Default: "UDP"
- **Backup OBP flag**: Determines whether or not the backup proxy is used as an outbound proxy.
  Value range: "Yes", "No"
  Default: "No"
- Network > Port Configuration > **Backup proxy**: Port of the backup proxy server.
  Default: 5060

## Administration via WBM

### System > Registration




### Network > Port configuration



### Administration via Local Phone

- Admin
  - System
    - Registration
      - SIP session
      - SIP survivability
        - **Backup reg. flag**
        - **Backup proxy addr.**
        - **Backup reg timer**
        - **Backup transport**
        - **OBP flag**

- Admin
  - Network
    - Port Configuration
      - **Backup proxy**

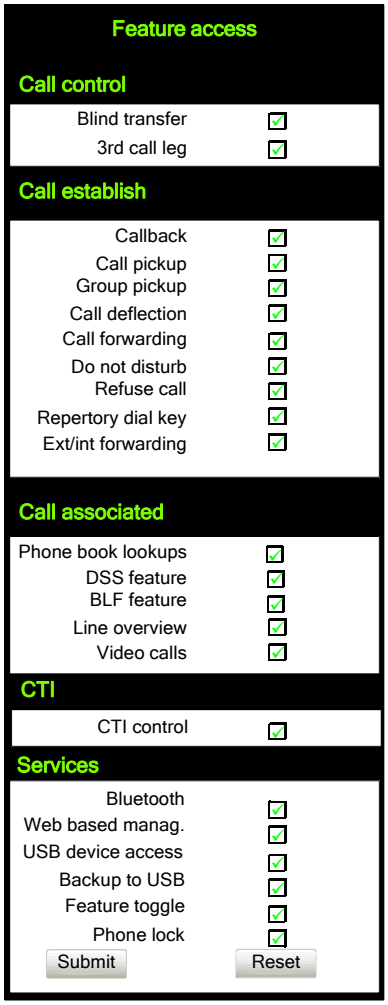
## 3.6 Feature Access

Certain OpenStage features and interfaces can be enabled or disabled:

- Blind transfer (see Section 3.8.9, “Blind Call Transfer / Move Blind”)
- 3rd call leg (consultation from a second call; see user manual)
- Callback busy (see Section 3.8.21, “Callback” and Section 3.7.6, “Callback URIs”)
- Callback no reply (see Section 3.8.21, “Callback” and Section 3.7.6, “Callback URIs”)
- Call pickup (see Section 3.8.20, “Directed Pickup”)
- Group pickup (see Section 3.8.16, “Group Pickup”)
- Call deflection (see Section 3.8.11, “Deflect a Call”)
- Call forwarding (see Section 3.8.4, “Call Forwarding (Standard)”)
- Do not disturb (see Section 3.8.15, “Do Not Disturb”)
- Refuse call (see Section 3.7.1, “Allow Refuse”)
- Repertory dial key (see Section 3.8.17, “Repertory Dial”)
- Ext/int forwarding (see Section 3.8.5, “Call Forwarding by Call Type”)
- Phone book lookups (see user manual)
- DSS feature (see Section 3.11.5, “Direct Station Select (DSS)”)
- BLF feature (see Section 3.8.28, “BLF Key”)
- Line overview (see user manual)
- Video calls (see user manual)
- Callback cancel (see Section 3.8.22, “Cancel Callbacks” and Section 3.7.6, “Callback URIs”)
- CTI control (see Section 3.7.11, “uaCSTA Interface”)
- Bluetooth (see Section 3.27, “Bluetooth (OpenStage 60/80)”)
- Web based manag. (see Section 1.6.1, “Web-based Management (WBM)”)
- USB device access (see user manual)
- Backup to USB (see user manual)
- Feature toggle (see Section 3.8.18, “Hunt Group: Send Busy Status”)
- Phone lock (see user manual)

## Administration via WBM

System > Features > Feature access




## Administration via Local Phone

- Admin
  - System
    - Features
      - Feature access
        - Call control
          - **Blind transfer**
          - **3rd call leg**

### Administration via Local Phone

- Admin
  - System
    - Features
      - Feature access
        - Call establish
          - **Callback**
          - **Call pickup**
          - **Group pickup**
          - **Call deflection**
          - **Call forwarding**
          - **Do not disturb**
          - **Refuse call**
          - **Repertory dial key**
          - **Ext/int forwarding**

- Admin
  - System
    - Features
      - Feature access
        - Call associated
          - **Phone book lookups**
          - **DSS feature**
          - **BLF feature**
          - **Line overview**
          - **Video calls**

- Admin
  - System
    - Features
      - Feature access
        - CTI
          - **CTI control**

- Admin
  - System
    - Features
      - Feature access
        - Services
          - **Bluetooth**
          - **Web based manag.**
          - **USB device access**
          - **Backup to USB**
          - **Feature toggle**
          - **Phone lock**

## 3.7 Feature Configuration

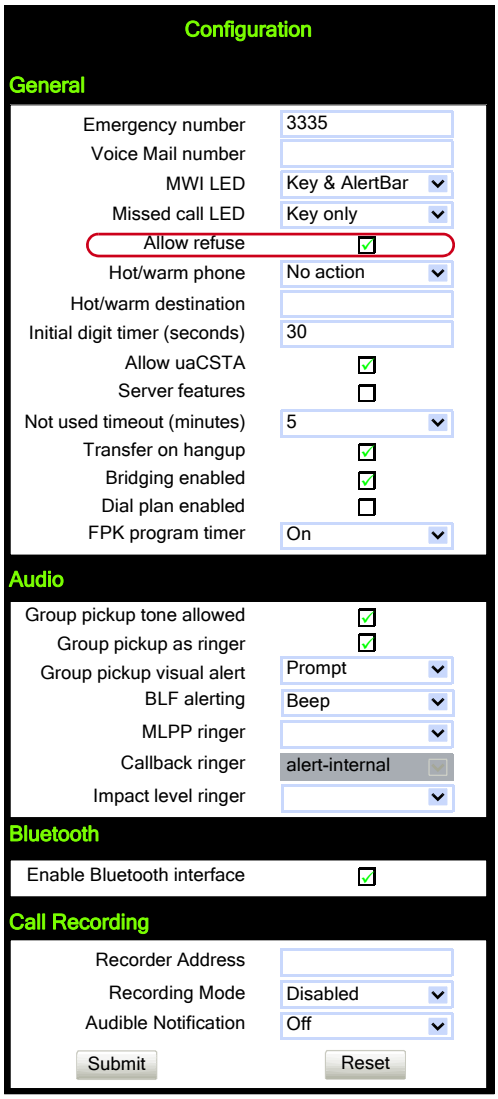
### 3.7.1 Allow Refuse

This parameter defines whether the Refuse Call feature is available on the phone. The possible values are "Yes" or "No". The default is "**Yes**".

This parameter can also be configured under System > Features > Feature access (see Section 3.6, “Feature Access”).

#### Administration via WBM

System > Features > Configuration



### Administration via Local Phone

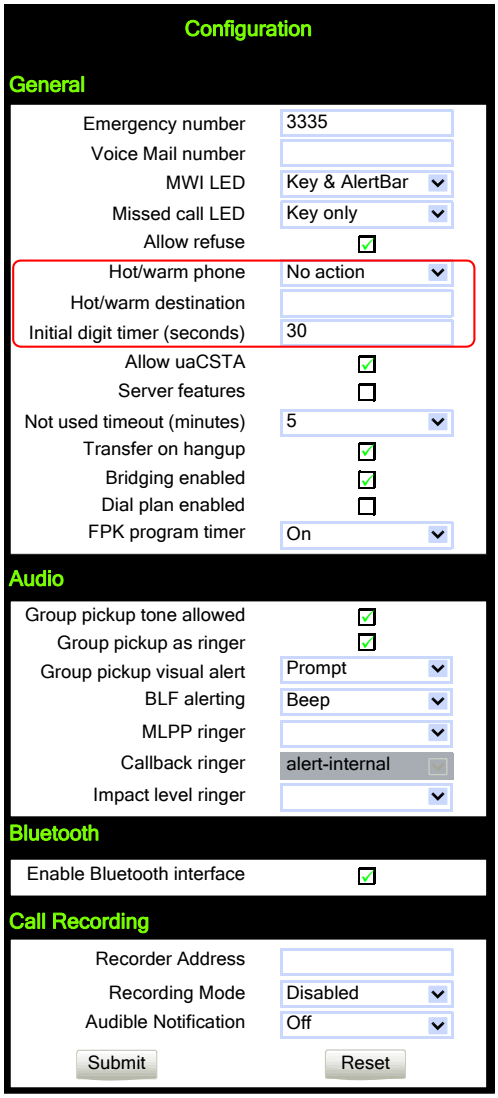
- Admin
  - System
    - Features
      - Configuration
        - General
          - **Allow refuse**

## 3.7.2 Hot/Warm Phone

If the phone is configured as hot phone, the number specified in **Hot warm destination** is dialed immediately when the user goes off-hook. For this purpose, **Hot warm phone** must be set to "Hot phone". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in **Initial digit timer (seconds)** (for details, see Section 3.7.3, “Initial Digit Timer”). During the delay period, the user can dial a number which will be used instead of the hot/warm destination. In addition, the user will be provided with a dial tone during the delay period. With the setting "No action", hot phone or warm phone functionality is disabled.

### Administration via WBM

System > Features > Configuration



### Administration via Local Phone

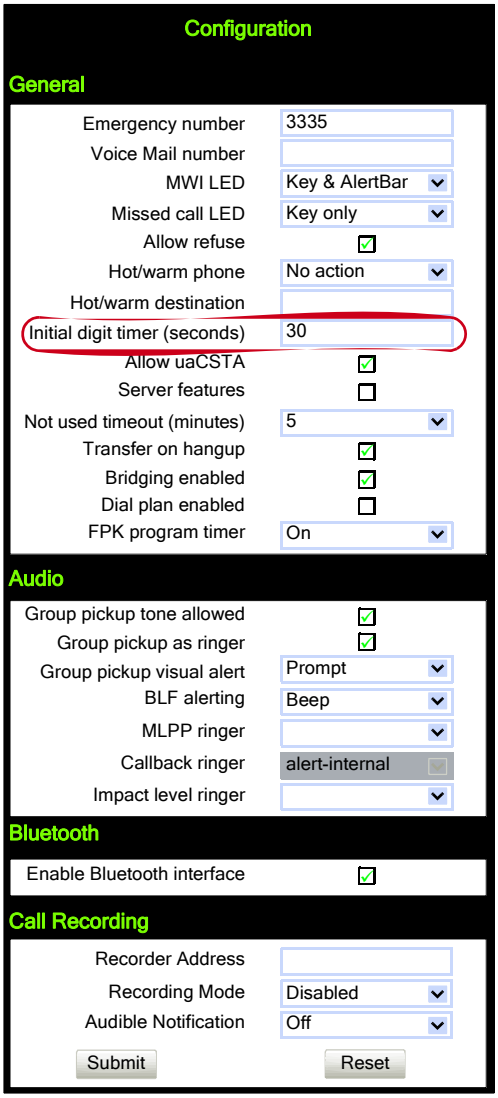
- Admin
  - System
    - Features
      - Configuration
        - General
          - **Hot / warm phone**
          - **Hot / warm destination**
          - **Initial digit timer**

## 3.7.3 Initial Digit Timer

This timer is started when the user goes off-hook, and the dial tone sounds. When the user has not entered a digit until timer expiry, the dial tone is turned off, and the phone changes to idle mode. The **Initial digit timer (seconds)** parameter defines the duration of this timespan.

### Administration via WBM

System > Features > Configuration




### Administration via Local Phone

└── Admin
  └── System
    └── Features
      └── Configuration
        └── General
          └── **Initial digit timer**

## 3.7.4 Group Pickup

This feature is only available when allowed under System > Features > Feature access (see Section 3.6, “Feature Access”).

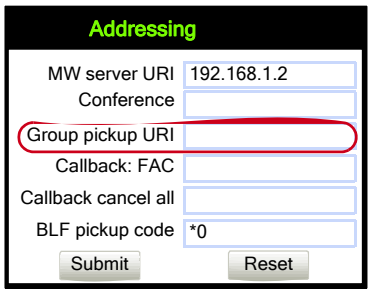
### 3.7.4.1 Feature Code

This feature allows a user to collect a call from any ringing phone that is in the same pickup group. To be a member of a Call Pickup group, the phone must be configured with the corresponding URI of the Call Pickup group service provided by the server. An example pickup URI is "**3".

#### Administration via WBM

The BLF pickup code parameter is only relevant when the phone is connected to an Asterisk server.

System > Features > Addressing




### 3.7.4.2 Pickup alert

If desired, an incoming call for the pickup group can be indicated acoustically.

The **Group pickup tone allowed** parameter activates or deactivates the generation of an acoustic signal for incoming pickup group calls. The default is "Yes". If this is activated, **Group pickup as ringer** determines whether the current ring tone or an alert beep is used. If set to "Yes", a pickup group call will be signaled by a short ring tone; the currently selected rigtone is used. If set to "No", a pickup group call will be signaled by an alert tone. The default is "Yes".

Depending on the phone state and the setting for **Group pickup as ringer**, the group pickup tone comes from the loudspeaker, the handset, or the headset. The volumes can be set in the local user menu, under Audio > Volumes.

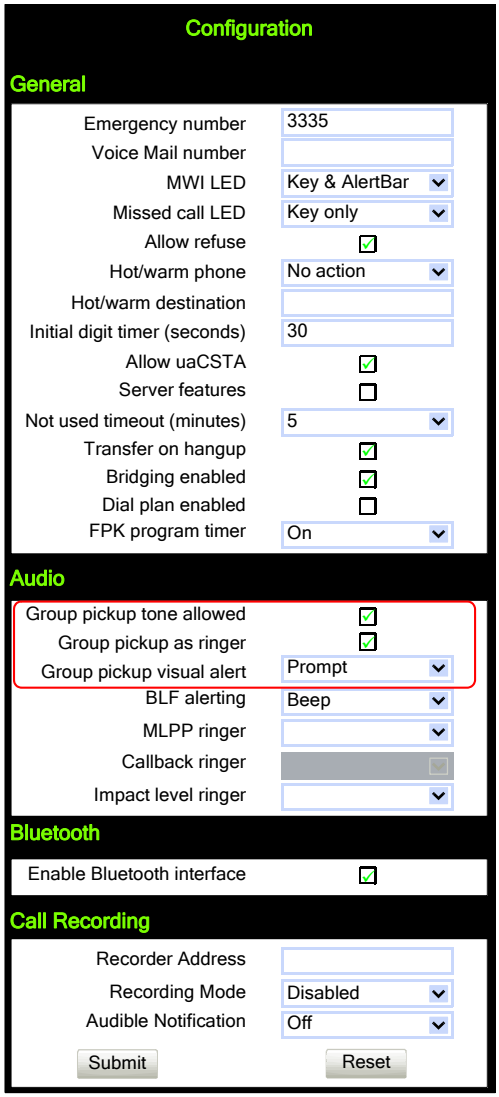
The following table shows the group pickup alert behaviour for each possible scenario:

| **Phone State** | | | **Group pickup as ringer=yes** | **Group pickup as ringer=no** |
|---|---|---|---|---|
| **Ringer on** | **Idle** | | Ring tone<br>Speaker | Beep<br>Speaker |
| | **In call** | **Handset** | Ring tone<br>Speaker | Beep<br>Handset |
| | | **Handset**<br>**Open listening** | Beep<br>Handset and Speaker | Beep<br>Handset and Speaker |
| | | **Headset** | Ring tone<br>Speaker | Beep<br>Headset |
| | | **Headset**<br>**Open listening** | Beep<br>Headset and Speaker | Beep<br>Headset and Speaker |
| | | **Hands-free** | Beep<br>Speaker | Beep<br>Speaker |
| **Ringer off** | **Idle** | | Nothing | Nothing |
| | **In call** | **Handset** | Nothing | Beep<br>Handset |
| | | **Handset**<br>**Open listening** | Beep<br>Handset and Speaker | Beep<br>Handset and Speaker |
| | | **Headset** | Nothing | Beep<br>Headset |
| | | **Headset**<br>**Open listening** | Beep<br>Headset and Speaker | Beep<br>Headset and Speaker |
| | | **Hands-free** | Beep<br>Speaker | Beep<br>Speaker |

**Group pickup visual alert** defines the user action required to accept a pickup call. If "Prompt" is selected, an incoming pickup call is signaled by an alert on the phone GUI. As soon as the user goes off-hook or presses the speaker key, the pickup call is accepted. Alternatively, the user can press the corresponding function key, if configured. If "Notify" is selected, an incoming pickup call is signaled by an alert on the phone GUI. To accept the call, the user must confirm the alert or press the corresponding function key, if configured.

## Administration via WBM

System > Features > Configuration




## Administration via Local Phone

└── Admin
  └── System
    └── Features
      └── Group pickup
        ├── **Group pickup tone**
        ├── **Group pickup as ringer**
        └── **Group pickup visual**

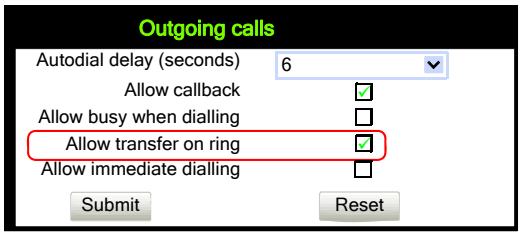
## 3.7.5 Call Transfer

### 3.7.5.1 Transfer on Ring

If this function is active, a call can be transferred after the user has dialled the third participant's number, but before the third party has answered the call. This feature is enabled or disabled in the User menu. The default is "Yes".

#### Administration via WBM (User menu)

User > Configuration > Outgoing calls




#### Administration via Local Phone (User menu)

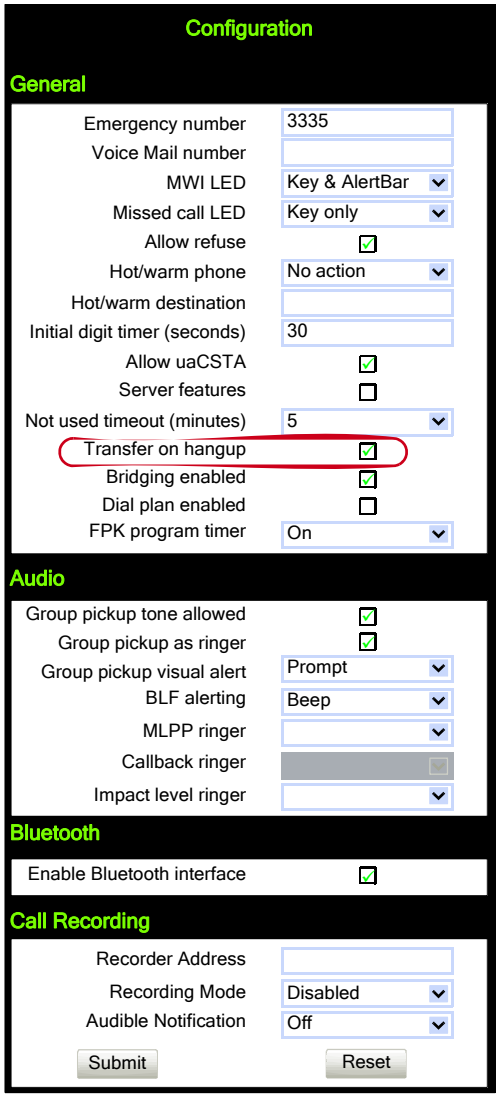
User
Configuration
Outgoing calls
**Transfer on ring**

### 3.7.5.2 Transfer on Hangup

This feature applies to the following scenario: While A is talking to B, C calls A. A accepts the call, so B is on hold and the call between A and C is active. If **Transfer on hangup** is enabled, and A goes on-hook, B gets connected to C. If disabled, C will be released when A hangs up, and A has the possibility to reconnect to B. By default, the feature is disabled.

## Administration via WBM

System > Features > Configuration




## Administration via Local Phone

└── Admin
  └── System
    └── Features
      └── Configuration
        └── General
          └── **Transfer on hangup**

## 3.7.6 Callback URIs

The Callback option allows the user to request a callback on certain conditions. The callback request is sent to the SIP server. The **Code for callback busy** requests a callback if the line is busy, i. e. if there is a conversation on the remote phone. **Code for callback no reply** applies when the call is not answered, i. e. if nobody lifts the handset or accepts the call in another way. The **Code for callback cancel all** all deletes all the callback requests stored previously on the telephone system/SIP server.

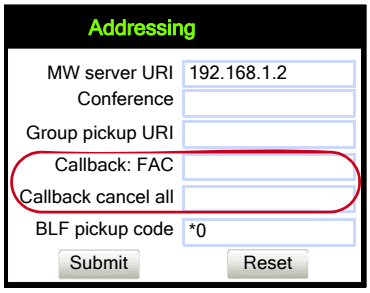
The callback feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

### Data required

- **Callback: FAC**: Access code that si sent to the server for all kind of Callback .
- **Code for callback cancel all** / **Callback: Cancel all**: Access code for canceling all call-back requests on the server.

### Administration via WBM

System > Features > Addressing




### Administration via Local Phone

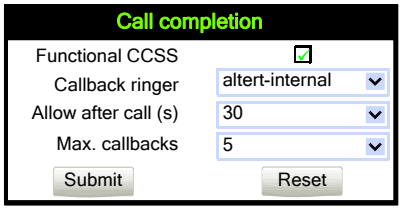
- Admin
  - System
    - Features
      - Addressing
        - **Callback: FAC**
        - **Callback: Cancel all**

### 3.7.6.1 Call Completion

Used with Asterisk only

#### Administration via WBM

System > Features > Call Completion




#### Administration via Local Phone

- Admin
  - System
    - Features
      - Call completion
        - **Functional CCSS**
        - **Callback ringer**
        - **Allow after call (s)**
        - **Max. callbacks**

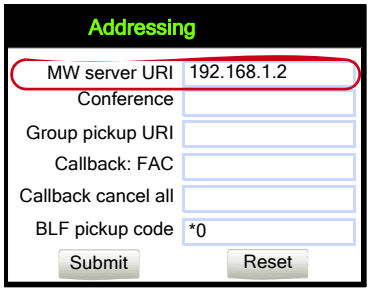
## 3.7.7 Message Waiting Address

The MWI (Message Waiting Indicator) is an optical signal which indicates that voicemail messages are on the server. Depending on the SIP server / gateway in use, the **Message waiting server address**, that is the address or host name of the server that sends message waiting notifications to the phone, must be configured.

With OpenScape Voice, this setting is not typically necessary for enabling MWI functionality.

### Administration via WBM

System > Features > Addressing




### Administration via Local Phone

Admin
System
Features
Addressing
**MWI server URI**

## 3.7.8 Indicate Messages

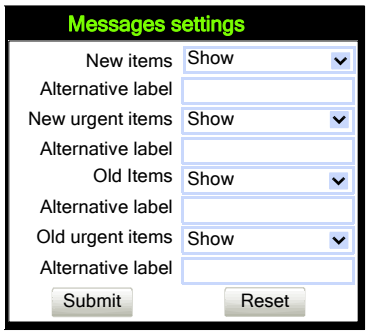
The indication of old and new messages on the display can be configured. There are 4 categories of voicemail messages: new, new urgent, old, and old urgent. For each category, the administrator can define whether the message count is shown or hidden, and set a header for the category. If all four settings on the form are set to "Hide", the VoiceMail summary screen is not shown to the user. Any other permutation of "Show/Hide" settings must result in a VoiceMail summary. If theVoiceMail summary is not shown then calling the mailbox will be a single-step process on a suitably configured OS80/60 and at least a two-step process on OS40/20/15.

### Data required

- **New items**: Determines whether new items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for new items.
- **New urgent items**: Determines whether new urgent items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for new urgent items.
- **Old items**: Determines whether new urgent items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for old items.
- **Old urgent items**: Determines whether old urgent items are indicated.
  Value range: "Show", "Hide"
- **Alternative label**: Label for old urgent items.

### Administration via WBM

Local functions > Messages settings



### Administration via Local Phone

- Admin
  - Locatl functions
    - Messages settings
      - **New items**
      - **Alternative label**
      - **New urgent items**
      - **Alternative label**
      - **Old items**
      - **Alternative label**
      - **Old urgent items**
      - **Alternative label**

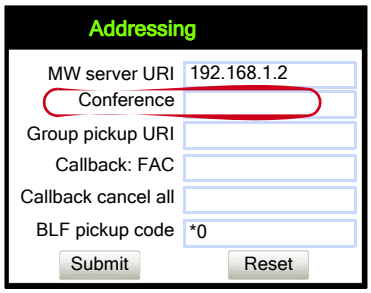
## 3.7.9 System Based Conference

The **Conference URI** provides the number/URI used for system based conferences, which can involve 3 to 16 members. This feature is not available with every system.

It is recommended not to enter the full URI, but only the user part. For instance, enter "123", not "123@<SIP SERVER ADDRESS>". A full address in this place might cause a conflict when Phone Administration uses multiple nodes.

### Administration via WBM

System > Features > Addressing



### 3.7.10 Server Based Features

Please note that the **Server features** parameter, despite the name similarity, is not related to the Server feature functionality as described in Section 3.8.27, “Server Feature”.

The use of server based call forwarding and server based DND is enabled or disabled here. When phone based DND and phone based call forwarding are to be used, **Server features** must be deactivated. This is the default setting. For using server based Call Forwarding or server based DND, it must be activated.

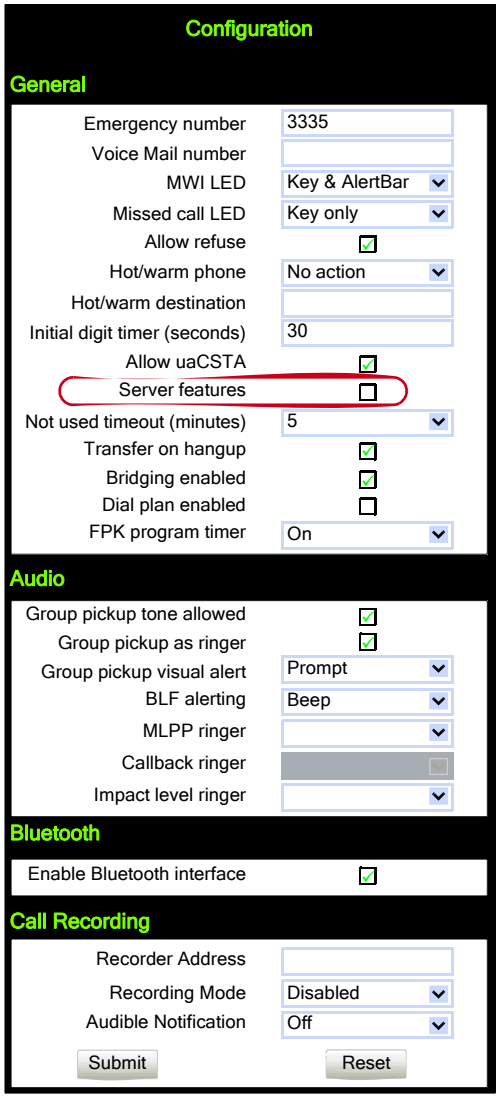
**Server features** is deactivated automatically if System > Registration > Server type (see Section 3.5.7, “SIP Registration”) is set to "HiQ8000".

Before switching **Server features** on or off, please ensure that both Call Forwarding and DND are not activated. Otherwise, the user will not be able to control the feature any more.
It is recommended to set **Server features** when setting up the phone, and avoid further changes, as possible.

To enable server based features, uaCSTA must be allowed (see Section 3.7.11, “uaCSTA Interface”).

## Administration via WBM

System > Features > Configuration




## Administration via Local Phone

Admin
System
Features
Configuration
General
**Server features**

## 3.7.11 uaCSTA Interface

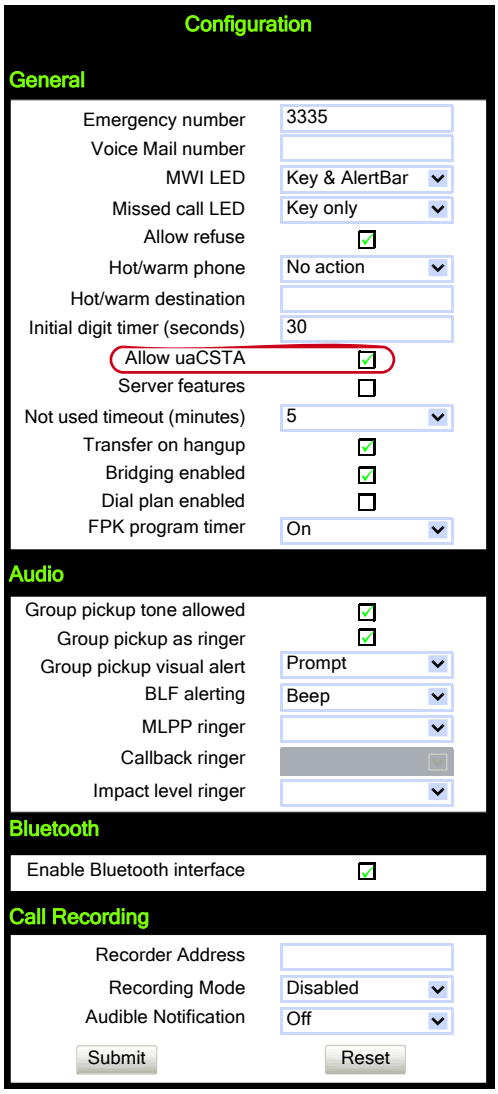
User Agent CSTA (uaCSTA) is a limited subset of the CSTA protocol, which allows external CTI applications to interact with the phone.

Access to the users “CTI calls” menu in User > Configuration > Incoming Calls can be allowed or disallowed (see Section 3.6, “Feature Access”).

If **Allow uaCSTA** is enabled, applications which support the uaCSTA standard will have access to the OpenStage phone. The default is "Yes".

### Administration via WBM

System > Features > Configuration



### Administration via Local Phone

- Admin
  - System
    - Features
      - Configuration
        - General
          - **Allow uaCSTA**

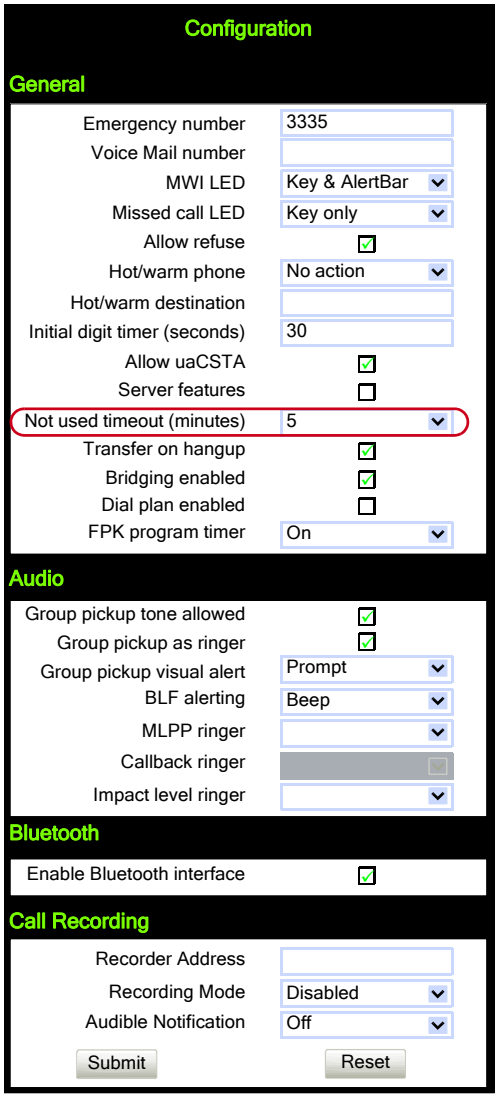
## 3.7.12 Local Menu Timeout

The timeout for the local user and admin menu is configurable. When the time interval is over, the menu is closed and the administrator/user is logged out. The timeout may be helpful in case a user does a long press on a line key unintentionally, and thereby invokes the key configuration menu. The menu will close after the timeout, and the key will return to normal line key operation. The timeout ranges from 1 to 5 minutes. The default value is 2.

The current position in the user or admin menu is kept in case the user/admin has exited the menu, e.g. for receiving a call. Thus, if the user/admin re-enters the menu, he is directed to exactly that submenu, or parameter, which he had been editing before.

### Administration via WBM

System > Features > Configuration



**Administration via Local Phone**

```
└--- Admin
     └--- System
          └--- Features
               └--- Configuration
                    └--- General
                         └--- Not used timeout
```

## 3.7.13 Call Recording

With firmware version V2R2, call recording is possible for OpenStage 15/20/40/60/80 using an " ASC Voice Recorder". The implementation is similar to a local conference, with the recording device acting as the third conference member. To start recording, the phone calls the recording device and provides it with the mixed audio data. Unlike a true local conference, the call leg used for recording can not transport audio from the recording device to the phone.

With the **Call recording mode**/**Recording Mode** parameter, the behaviour of the feature is determined:

- "Disabled": Recording is not possible.
- "Manual": The user starts and stops recording manually using the menu or a free programmable key.
- "Auto-start": The recording starts automatically; besides, the user can stop and start the recording manually.
- "All Calls": The recording starts automatically for all recordable calls; the user can not stop or start the recording manually.

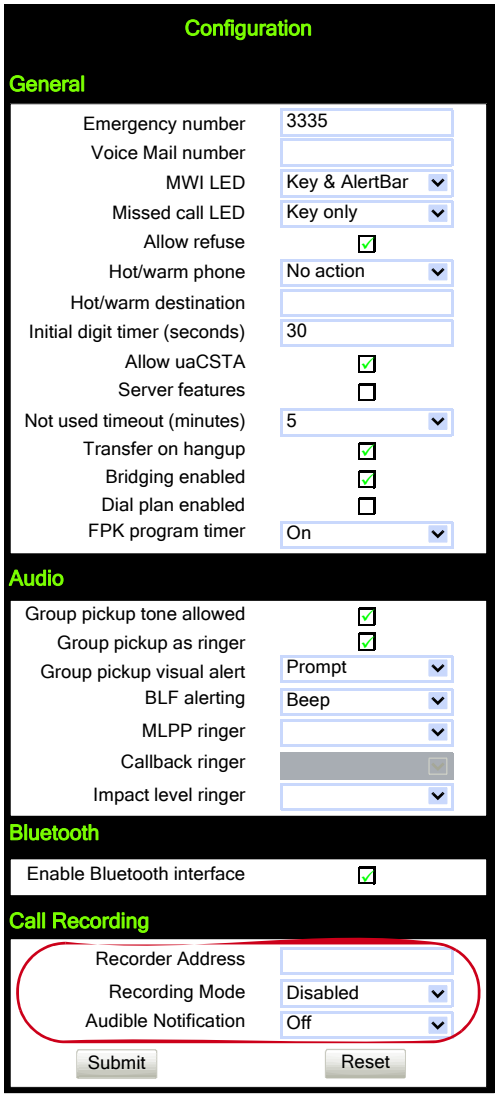
The **Audible indication**/**Audible Notification** parameter determines if and how the parties in a call are informed when a call is being recorded:

- "Off": No audible indication is given.
- "Single-shot": A single audible indication is given when recording commences or resumes.
- "Repeated": An audible indication is given when recording commences or resumes, and repeated periodically during the recording.

With the Recorder Address/Recorder number parameter, the SIP address of the call recorder is specified.

## Administration via WBM

System > Features > Configuration




## Administration via Local Phone

- Admin
  - System
    - Features
      - Configuration
        - Call Recording
          - **Recorder number**
          - **Recorder mode**
          - **Audible notification**

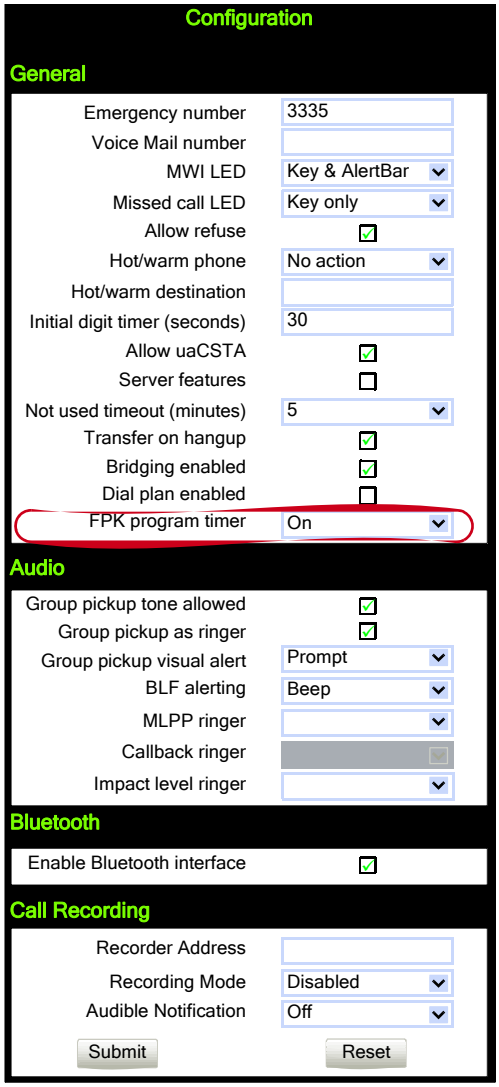
## 3.8 Free Programmable Keys

OpenStage 15/40/60/80 phones feature free programmable keys (FPKs) which can be associated with special phone functions. In the Administrator pages of the WBM, the programmable keys menu can be accessed via System > Features > Program keys.

At the phone, the configuration menu for a specific key is called by a long press on the related key. This feature can be disabled by deactivating the **FPK program timer**. When this parameter is disabled, it is not possible to enter programming mode by long key press. However, the other methods for key programming remain enabled. The functions available and their parameters are described in the following sub-sections. For keyset and DSS functionality, please refer to Section 3.11, “Multiline Appearance/Keyset”.

### Administration via WBM

System > Features > Configuration > General



**Administration via Local Phone**

└--- Admin
└--- System
└--- Features
└--- Configuration
└--- General
└--- **FPK prog. timer**

## 3.8.1 Clear (no feature assigned)

The label displayed to the left of the key is defined in **Key label <key number>**.

**Administration via WBM**

System > Features > Program keys

## 3.8.2 Selected Dialing

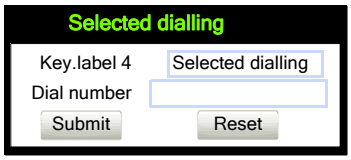
On key press, a pre-defined call number is called.

The label displayed to the left of the key is defined in **Key label <key number>**.

The call number defined in the **Dial number** parameter is dialed on key press.

**Administration via WBM**

System > Features > Program keys > Selected dialling



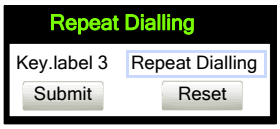
## 3.8.3 Repeat Dialing

On key press, the call number that has been dialed lastly is dialed again.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Repeat dialling




## 3.8.4 Call Forwarding (Standard)

This key function controls phone based call forwarding. If forwarding is enabled, the phone will forward incoming calls to the predefined call number, depending on the current situation.

To use phone based call forwarding, **Server features** must be switched off (see Section 3.7.10, “Server Based Features”).

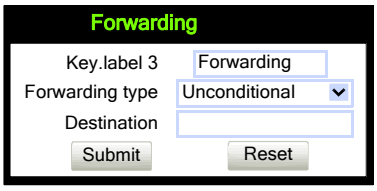
This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

The **Forwarding type** parameter determines the forwarding behaviour. If "Unconditional" is selected, any incoming call will be forwarded. If "On no reply" is set, the call will be forwarded when the user has not answered within a specified timespan. The timespan is configured in the WBM user pages under User > Configuration > Incoming calls > Forwarding > No reply delay (seconds). If "On busy" is selected, incoming calls will be forwarded when the phone is busy.

### Administration via WBM

System > Features > Program keys > Forwarding



## 3.8.5 Call Forwarding by Call Type

This feature enhances the Call Forwarding (Standard) operation (see Section 3.8.4, “Call Forwarding (Standard)”) by adding support for additional Call Forwarding settings explicitly for External and Internal calls, as well as the existing capability to forward any call, using functional menus that extend the existing Call Forwarding UI.

To use extended call forwarding, **Server features** and **Allow uaCSTA** must be switched on (see Section 3.7.10, “Server Based Features”).

This feature can be enabled or disabled under System > Features > Feature access > Ext/int forwarding (see Section 3.6, “Feature Access”).

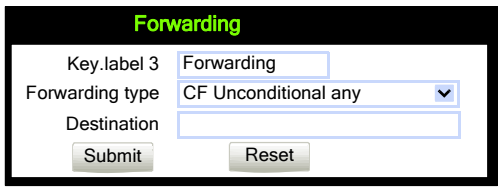
The label displayed to the left of the key is defined in **Key label <key number>**. It is possible to have an extra key defined for each Call Forwarding Call Type.

### Data required

- **Forwarding type**: Determines forwarding behaviour.
  Value range: „CF Unconditional any“,
  „CF no reply - any“,
  „CF busy - any“,
  „CF unconditional - ext.“,
  „CF unconditional - int.“,
  „CF no reply - ext.“,
  „CF no reply - int.“,
  „CF busy - ext.“,
  „CF busy - int“
  Default: „CF Unconditional any“
- **Destination**: Destination number of call forwarding.

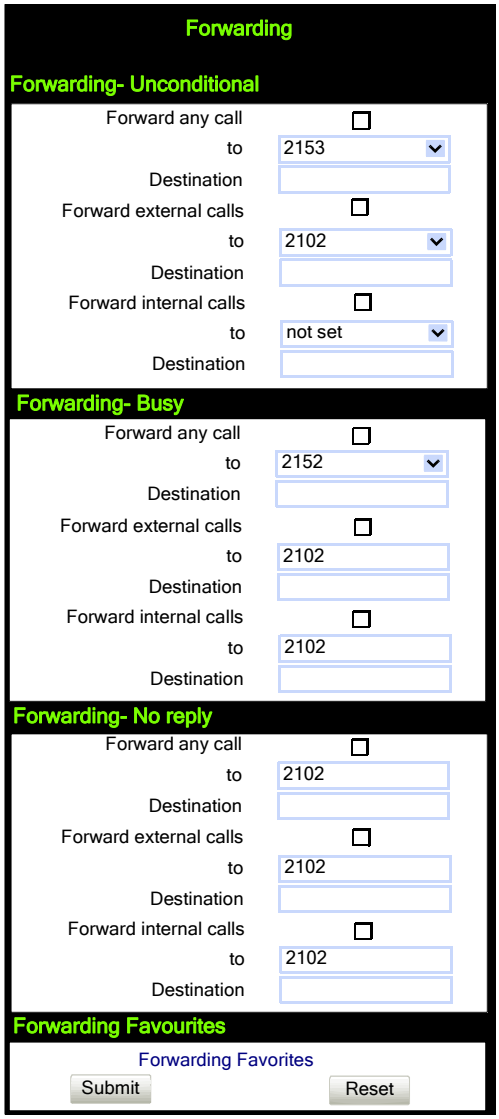
### Administration via WBM

System > Features > Program keys > Forwarding



## Administration via WBM (User menu)

User > Configuration > Incoming calls > Forwarding



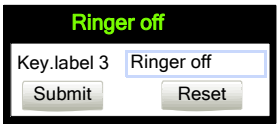
### 3.8.6 Ringer Off

Turns off the ring tone. Incoming calls are indicated via LEDs and display only.

The label displayed to the left of the key is defined in **Key label <key number>**.

#### Administration via WBM

System > Features > Program keys > Ringer off




### 3.8.7 Hold

The call currently selected or active is put on hold.

A held call can be retrieved by pressing the key a second time.

The label displayed to the left of the key is defined in **Key label <key number>**.

#### Administration via WBM

System > Features > Program keys > Hold

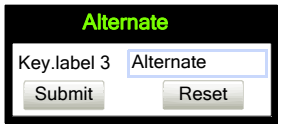
### 3.8.8 Alternate

Toggles between two calls; the currently active call is put on hold.

The label displayed to the left of the key is defined in **Key label <key number>**.

#### Administration via WBM

System > Features > Program keys > Alternate



## 3.8.9 Blind Call Transfer / Move Blind

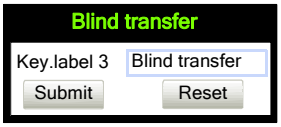
A call is transferred without consultation, as soon as the phone goes on-hook or the target phone goes off-hook.

> This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Blind transfer



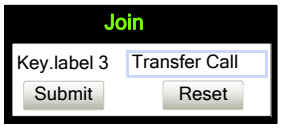

## 3.8.10 Transfer Call

Call transfer, applicable when there is one active call and one call on hold. The active call and the held call are connected to each other, while the phone that has initiated the transfer is disconnected.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Transfer Call



## 3.8.11 Deflect a Call

On key press, an incoming call is deflected to the specified destination.

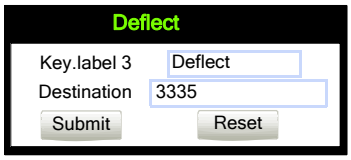
> This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

The target destination is defined in the **Destination** parameter.

### Administration via WBM

System > Features > Program keys > Deflect



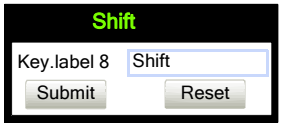

## 3.8.12 Shift Level

Shift the level for the programmable keys. When activated, the functions assigned to the shifted level are available on the keys.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Shift



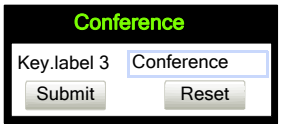

## 3.8.13 Phone-Based Conference

Establishes a three-party conference from an active call and held call.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Conference




## 3.8.14 Accept Call via Headset (OpenStage 40/60/80)

On key press, an incoming call is accepted via headset.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Headset

## 3.8.15 Do Not Disturb

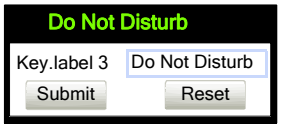
If this feature is activated, incoming calls will not be indicated to the user.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Do Not Disturb



## 3.8.16 Group Pickup

On key press, a call for a different destination within the same pickup group is answered.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Group pickup

## 3.8.17 Repertory Dial

This feature is similar to the selected dialing function, but additionally, special calling functions are possible. The desired number and/or function is selected via the **Dial string** parameter.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

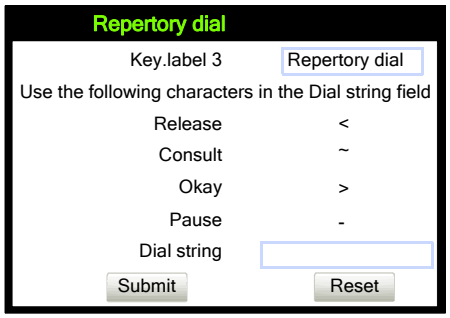
The following call functions are available:

- "<" disconnect a call.
- "~" start a consultation call. Example: "~3333>"
- ">" (preceded by a call number) start a call. Example: "3333>"
- "-" enter a pause, e. g. for exit-code or international dialing. Example: "0-011511234567>"

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Repertory dial



## 3.8.18 Hunt Group: Send Busy Status

This feature is relevant for hunt groups. If the user is a member of a hunt group and wants another member of the hunt group to pick up an incoming call, he can signal Busy status using the Feature toggle function.

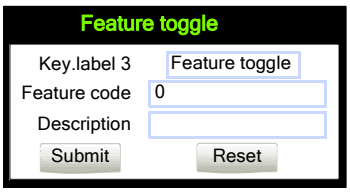
This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

The **Feature code** parameter is the OpenScape Voice code for Busy status. In the **Description** field, an appropriate description for the feature can be entered.

### Administration via WBM

System > Features > Program keys > Feature toggle



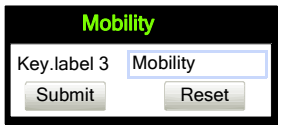

## 3.8.19 Mobile User Logon

The mobility feature enables users to transfer their personal settings, such as their key layout, or personal phonebook, from one phone to another. The data is stored and managed by the DLS (Deployment Service).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Mobility



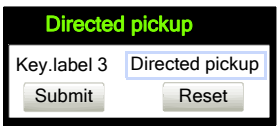
## 3.8.20 Directed Pickup

This feature enables the user to pick up a call which is ringing at another phone. On pressing the key, a menu opens which requests the call number of the target phone.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Directed pickup




## 3.8.21 Callback

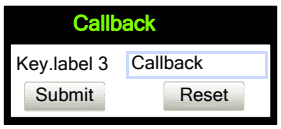
When the remote phone called is busy does not reply, the user can send a callback request to the server by pressing this key.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Callback



## 3.8.22 Cancel Callbacks

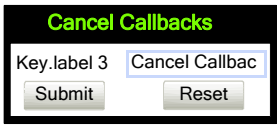
With this this function, the user can cancel all callback requests on the server.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Cancel callbacks



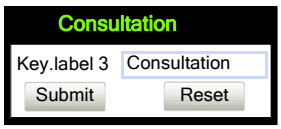

## 3.8.23 Consultation

When the phone is engaged in an active call, this function opens a dialing menu to make a consulation call.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Consultation




## 3.8.24 Call Waiting

Enables or disables the call waiting feature. If enabled, calls from a third party are allowed during an active call.

The Call Waiting feature cannot be disabled if System > Registration > Server type (see Section 3.5.7, “SIP Registration””) is set to "HiQ8000".

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Call waiting

## 3.8.25 Call recording

Starts or stops call recording (for configuring call recording, see Section 3.7.13, “Call Recording”).

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Call Recording

## 3.8.26 Auto Answer With Zip Tone

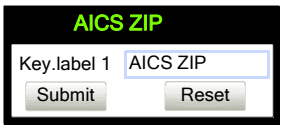
This feature is primarily designed for call centers. If activated, and a headset is used, the phone will automatically accept incoming calls without ringing and without the necessity to press a key. Moreover, additional signalling information from Phone Administration is not required.

To indicate a new call to the user, a zip tone is played through the headset when the call is accepted.

The feature is available for OpenStage 40/60/80, which provide a headset jack; it only operates if the headset is plugged in. In case the key for feature activation has been pressed before the headset is connected, the feature will be automatically activated when the headset is plugged in.

**Administration via WBM**

System > Features > Program keys > AICS Zip tone




## 3.8.27 Server Feature

Invokes a feature on the SIP server. The status of the feature can be monitored via the LED associated to the key.

This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the Administration Manual for OpenStage 15/20/40/60/80 on Asterisk.

## 3.8.28 BLF Key

This function offers the possibility to monitor another extension, and to pick up calls for the monitored extension.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

This function is intended primarily for operation with an Asterisk SIP server. For details, please refer to the Administration Manual for OpenStage 15/20/40/60/80 on Asterisk.

## 3.8.29 Start Application

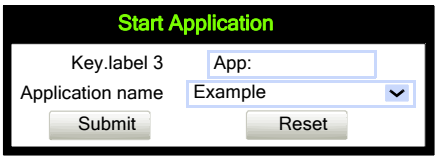
With this key, the user can start a pre-defined XML application (see Section 3.19, “Applications”). XML applications are available for OpenStage 60/80 phones.

The label displayed to the left of the key is defined in **Key label <key number>**.

The **Application name** parameter selects the XML application to be started.

### Administration via WBM

System > Features > Program keys




## 3.8.30 Send Request via HTTP/HTTPS

With this function, the phone can send a specific HTTP or HTTPS request to a server. The function is available at any time, irrespective of registration and call state. Possible uses are HTTP-controlled features on the system, or functions on a web server that can only be triggered by HTTP/HTTPS request, e. g. login/logout for flexible working hours.

The **Protocol** parameter defines whether HTTP or HTTPS is to be used for sending the URL to the server.

The **Web server address** is the IP address or DNS name of the remote server to which the URL is to be sent.

The **Port** is the target port at the server to which the URL is to be sent.

The **Path** is the server-side path to the desired function, i. e. the part of the URL that follows the IP address or DNS name. Example: `webpage/checkin.html`

In the **Parameters** field, one or more key/value pairs in the format `"<key>=<value>"` can be added to the request, separated by an ampersand (`&`).
Example: `phonenumber=3338&action=huntGroupLogon`

The question mark will be automatically added between the path and the parameters. If a question mark has been entered at the start of the parameters, it will be stripped off automatically.

The **Method** parameter determines the HTTP method to be used, which can either be GET or POST. If GET is selected, the additional parameters (**Parameters**) and the user id/password (**Web server user ID**/**Web server password**) are part of the URL. If POST is selected, these data form the body of the message.

In case the web server requires user authentication, the parameters **Web server user ID** and **Web server password** can be used. If not null, the values are appended between the server-side path (**Path**) and the additional parameters (**Parameter**).

If the **LED controller URI** is given, the LED associated with this key indicates the state of the call number or SIP URI specified, provided the SIP server sends a notification:

- Busy notification: LED is glowing.
- Ringing notification: LED is blinking.
- Idle notification (state=terminated): LED is dark.

When assigning the function described here to the release key ⮐, please consider that this key has no LED.

With firmware version V2R2, the **Push support** parameter is available. If activated, the LED is controllable by a combination of an HTTP push request and an XML document. For further information, see the XML Applications Developer's Guide.

If you want to use the HTTP push solution, please ensure that the **LED controller URI** field is empty. Otherwise, the phone will only use the SIP mechanism for LED control, and ignore the push request.

The **Symbolic name** is used to assign a push request from the application server to the appropriate free programmable key resp. fixed function key. This value must be unique for all keys involved.

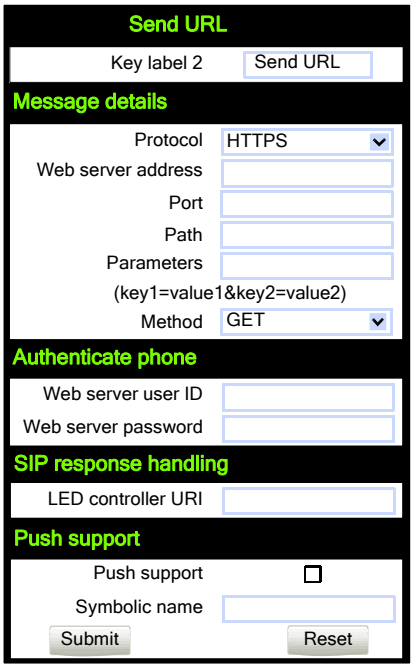
**Data required**

- **Key label <n>**: Label for the key.
- **Protocol**: Transfer protocol to be used.
  Value range: "HTTP", "HTTPS"
- **Web server address**: IP address or DNS name of the remote server.
- **Port**: Target port at the server.
- **Path**: Server-side path to the function.
- **Parameters**: Optional parameters to be sent to the server.
- **Method:** HTTP method used for transfer.
  Value range: "GET", "POST"
- **Web server user ID**: User id for user authentication at the server.
- **Web server password**: Password for user authentication at the server.

- **LED controller URI:** Indicates the state of the call number specified.
- **Push support** : Enables or disables LED control by push requests from the server.
- **Symbolic name** : Assigns a push request to the appropriate free programmable key resp. fixed function key.

### Administration via WBM

System > Features > Program keys > Send URL



## 3.8.31 Built-in Forwarding

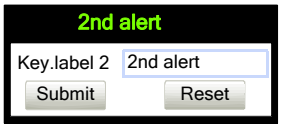
As a programmable key function, this is relevant for OpenStage 15 phones, which have no fixed forwarding key.

System > Features > Program keys

## 3.8.32 2nd Alert

This function allows for monitoring and accepting a second incoming call. When a call is ringing while the user is dialing, the LED will light up. As soon as the user presses the key, information about the incoming call is presented, and the user can accept the call. If a call is ringing, and another call starts ringing shortly after, the LED will light up, and the user has the possibility to toggle between these calls via key press.

System > Features > Program keys




## 3.8.33 Start Phonebook (OpenStage 40/15 only)

These key functions opens a menu which enables the user to start the personal or the corporate phonebook. For further information about the personal and corporate phonebook, please refer to the user guide for OpenStage 40/15 phones. For more information about the corporate phonebook, please see Section 3.17, “Corporate Phonebook: Directory Settings”.

### Administration via WBM

System > Features > Program keys > Personal directory

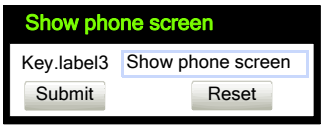
System > Features > Program keys > Corporate directory

## 3.8.34 Show phone screen (OpenStage 15 and OpenStage 40 only)

On pressing this key, the phone display switches to call view mode.

### Administration via WBM

System > Features > Program keys > Show phone screen

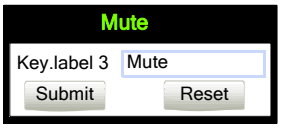



## 3.8.35 Mute (OpenStage 15 only)

On pressing this key, the microphone is turned off. This programmable key function is available only for OpenStage 15 phones, which have no fixed mute key.

### Administration via WBM

System > Features > Program keys > Mute

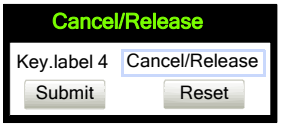



## 3.8.36 Release (OpenStage 15 only)

On pressing this key, the current call is disconnected. This programmable key function is available only for OpenStage 15 phones, which have no fixed release key.

### Administration via WBM

System > Features > Program keys > Release



## 3.9 Preset Function Keys (OpenStage 40 US only)

The OpenStage 40 US telephone comes with six programmable lit sensor keys, preset to the following factory settings:

- Shift
- Phonebook
- Group pickup
- Call Forward
- DND
- Show phone

All of this can be programmed on two separate levels but if you reset the phone, the keys in the first level will be reset to the default factory settings.

## 3.10 Fixed Function Keys

For

- OpenStage 60/80
  - the forwarding key, the release key, and the voice recognition key,
- OpenStage 20 and OpenStage 40
  - the release key, the redial key and the forwarding key

specific SIP or HTTP based functions can be defined. These functions can be employed as an alternative to the built-in functions.

### 3.10.1 Fixed Function Keys on OpenStage 40 US

For the Conference key, the Transfer key, and the Hold key, specific SIP or HTTP based functions can be defined. If you reset the phone, these three keys will be reset to the default factory settings.

## 3.11 Multiline Appearance/Keyset

This feature is available only on OpenStage 15, OpenStage 40 and OpenStage 60/80 phones.

A phone that has more than one line associated to it, and therefore works as a multiline phone, is referred to as "keyset". The lines are assigned to the phone by setting up a separate line key for each line.

The multiline appearance feature allows for multiple lines to be assigned to a keyset and for a line to be assigned to multiple keysets. This feature requires configuration in Phone Administration and in the telephone, and is particularly useful for executive-assistant arrangements.

In order to configure the phone as a keyset, it is required to

- use an outbound proxy (System > SIP interface > Outbound proxy, see Section 3.5.8.1, “Outbound Proxy”), and
- set the server type to "OS Voice" (System > Registration > Server type, see Section 3.5.7, “SIP Registration”).

For each keyset, a Primary Line/Main DN is required. The primary line is the dialing number for that keyset.

There are two types of line:

- **Private line**: A line with restricted line status signaling towards OSV.
- **Shared line**: A line that is shared between keysets.

### 3.11.1 Line key configuration

System > Features > Program keys

It is recommended to configure primary lines only on keys 1 to 6, or 1 to 5, if a shift key is needed. This ensures that the lines are still accessible when the user migrates to a different phone with fewer keys via the mobility feature.

A line corresponds to a SIP address of record (AoR), which can have a form similar to an E-mail address, or can be a phone number. It is defined by the **Address** parameter. For registration of the line, a corresponding entry must exist on the SIP server resp. the SIP registrar server.

A label can be assigned to the line key by setting its **Key label**.

Every keyset must necessarily have a line key for the primary line. To configure the key of the primary line, set **Primary line** to "true".

If **Ring on/off** is checked, the line will ring when an incoming call occurs, and a popup will appear on the display. If the option is not checked, the incoming call will be indicated only by the blinking of the key's LED. If it is desired that the line ring with a delay, the time interval in seconds can be configured by **Ring delay**.

When the user lifts the handset in order to initiate a call, the line to be used is determined by selection rules. To each line, a priority is assigned by the **Selection order** parameter. A line with the rank 1 is the first line to be considered for use. If more than one line have the same rank, the selection is made according to the key number. Note that **Selection order** is a mandatory setting; it is also relevant to the **Terminating line preference**, as well as to other functions.

The **Address** (Address of Record) parameter is the phone number resp. SIP name corresponding to the entry in the SIP registrar at which the line is to be registered.

For the configuration of line keys, the use of the DLS (Deployment Service) is recommended. For operating the DLS, please refer to the DLS user's guide. Alternatively, the web interface or the local menu can be used. Note that the creation of a new line key and the configuration of some parameters can not be accomplished by the phone's local menu.
Generally, it is advisable to restrict the user's possibilities to modify line keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

The **Realm**, a protection domain used for authenticated access to the SIP server, works as a name space. Any combination of user id and password is meaningful only within the realm it is assigned to. The other parameters necessary for authenticated access are **User Identifier** and **Password**. For all three parameters, there must be corresponding entries on the SIP server.

The **Shared type** parameter determines whether the line is a shared line, i. e. shared with other endpoints, or a private line, i .e. available exclusively for this endpoint. A line that is configured as primary line on one phone can be configured as secondary line on other phones.

Shared lines are not available if System > Registration > Server type (see Section 3.5.6, “SIP Registration”) is set to "HiQ8000".

When **Allow in overview** is set to "Yes", the line will be visible in the line overview on the phone's display.

Line overwiew can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”)

If a line is configured as hot line, the number indicated in **Hot warm destination** is dialed immediately when the user goes off-hook. This number is configurerd in the user menu under **Configuration > Keyset > Lines > Hot/warm destination**. To create a hot line, **Hot warm ac-**

**tion** must be set to "hot line". If set to "Warm phone", the specified destination number is dialed after a delay which is defined in **Initial digit timer (seconds)** (for details, see Section 3.7.3, “Initial Digit Timer”). During the delay period, it is possible for the user to dial a different number which will be used instead of the hot/warm line destination. In addition, the user will be provided with a dial tone during the delay period. With the setting "No action", the line key will not have hot line or warm line functionality.

System > Features > Program keys

### Data required

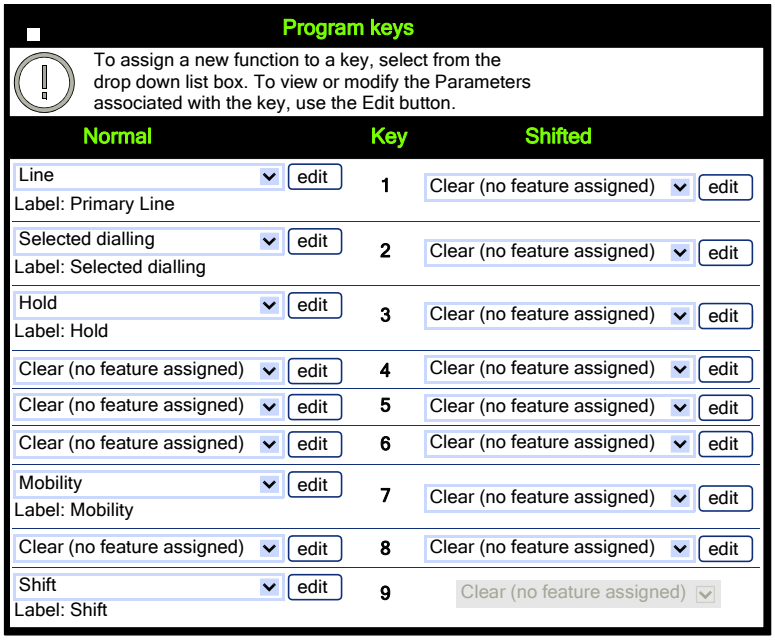
- **Key label <n>**: Set the label of the line key with the key number <n>.
  Default: "Line"
- **Primary line**: Determines whether the line is the primary line.
  Value range: "Yes", "No"
  Default: "No"
- **Ring on/off**: Determines whether the line rings on an incoming call.
  Value range: "On", "Off"
  Default: "On"
- **Ring delay (seconds)**: Time interval in seconds after which the line starts ringing on an incoming call.
  Default: 0
- **Selection order**: Priority assigned to the line for the selection of an outgoing line.
  Default: 0
- **Address**: Address/phone number which has a corresponding entry on the SIP server/ registrar.
- **Realm**: Domain wherein user id and password are valid.
- **User Identifier**: User name for authentication with the SIP server.
- **Password**: Password for authentication with the SIP server.
- **Shared type**: Determines whether the line is a shared line (shared by multiple endpoints) or a private line (only available for this endpoint).
  Value range: "shared", "private", "unknown".
  Default: "shared"
- **Allow in Overview**: Determines whether the line appears in the phone’s line overview.
  Value range: "Yes", "No"
  Default: "Yes"
- **Hot warm action** : Determines if the line is a regular line, a hot line, or a warm line.
  Value range: "No action", "hot line", "warm line"
- **Hot warm destination** : The destination to be dialed from the hot/warm line when the user goes off-hook.

A new line key can only be added by use of the WBM or, preferably, the DLS. Once a line key exists, it can also be configured by the local menu.

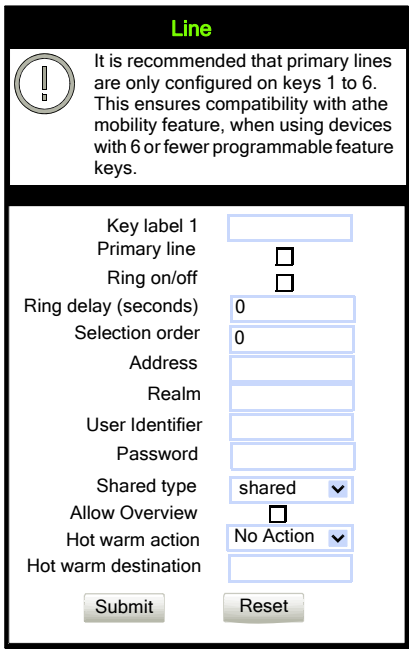
## Administration via WBM

1. Invoke the "Phone keys" dialog and select "line" in the pulldown menu of the key you want to configure. Next, click the **edit** button.

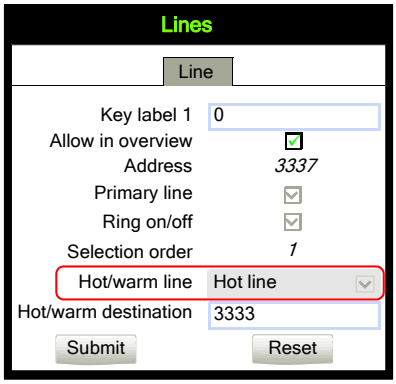
System > Features > Program keys



2. In the "Line" dialog, set the specific parameters for the line key.




3. (Only relevant if hot line / warm line is to be configured:) The destination for hot line or warm line is set in User menu > Configuration > Keyset > Lines:




In the local menu, the menu path is the same.

### Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via Web interface or DLS before.

- Admin
  - System
    - Features
      - Configuration
        - Keyset lines
          - Details For Keyset Line <xx>
            - **Address**
            - **Ring on/off**
            - **Selection order**
            - **Hot/warm action**

## 3.11.2 Configure Keyset Operation

The following parameters provide general settings which are common for all keyset lines.

The **Rollover ring** setting will be used when, during an active call, an incoming call arrives on a different line. If "no ring" is selected, the incoming call will not initiate a ring. If "alert ring" is selected, a 3 seconds burst of the configured ring tone is activated on an incoming call; "alert beep" selects a beep instead of a ring tone. "Standard ring tone" selects the default ringer.

**LED on registration** determines whether the line LEDs will be lit for a few seconds if they have been registered successfully with the SIP server on phone startup.

The **Originating line preference** parameter determines which line will be used when the user goes off-hook or starts on-hook dialing.

When a terminating call exists, the terminating line preference takes priority over originating line preference.

The following preferences can be configured:

- "idle line": An idle line is selected. The selection is based on the **Hunt ranking** parameter assigned to each line (see Section 3.11.1, “Line key configuration”).
- "primary": The designated Primary Line/Main DN is always selected for originating calls.
- "last": The line selected for originating calls is the line that has been used for the last call (originating or terminating).
- "none": The user manually selects a line by pressing its line key before going off-hook or by pressing the speaker key, to originate a call.

**Manual line selection overrides automatic line preferences.**

The **Terminating line preference** parameter decides which terminating line, i. e. line with an incoming call, is selected when the user goes off-hook.

The following preferences can be configured:

- "ringing line": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. In the case of multiple lines alerting or ringing, the lines are selected on the one that has been alerting the longest.
- "ringing PLP": The line in the alerting or audible ringing state is automatically selected when the user goes off-hook. However, if the prime line is alerting, it is given priority.
- "incoming": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected.
- "incoming PLP": The earliest line to start audible ringing is selected, or else the earliest alerting (ringing suppression ignored) line is selected. However, if the prime line is alerting, it is given priority.
- "none": To answer a call, the user manually selects a line by pressing its line key before going off-hook, or by pressing the speaker key.

**Manual line selection overrides automatic line preferences.**

**Line action mode** determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. The user has two options: 1) to reconnect to the remote phone by pressing the line key that corresponds to that call, or 2) to initiate another call from the newly selected line. If "release" is selected, the previously established call is ended.

If **Show focus** is checked, the LED of a line key flutters when the line is in use. If it is not checked, the line key is lit steady when it is in use.

The **Reservation timer** sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. The reservation of a line is accomplished by the Phone Administration server, which notifies all the endpoints sharing this line. If set to 0, the reservation timer is deactivated.

**Forward indication** activates or deactivates the indication of station forwarding, i. e. the forwarding function of Phone Administration. If **Forward indication** is activated and station forwarding is active for the corresponding line, the LED of the line key blinks.

**Preselect mode** determines the phone's behaviour when a call is active, and another call is ringing. If the parameter is set to "Single button", the user can accept the call a single press on the line key. If it is set to "Preselection", the user must first press the line key to select it and then press it a second time to accept the call. In both cases, the options for a ringing call are presented to the user: "Accept", "Reject", "Deflect".

**Preselect timer** is relevant if **Preselect mode** is set to "Preselection". The parameter sets the timeout in seconds for the second key press that is required to accept the call. After the timeout has expired, the call is no longer available.

When **Bridging enabled** (Admin > Features > Configuration) is activated, the user may join into an existing call on a shared line by pressing the corresponding line key. On key press, the Phone Administration builds a server based conference from the existing call parties and the user. If the call has already been in a server based conference, the user is added to this conference.

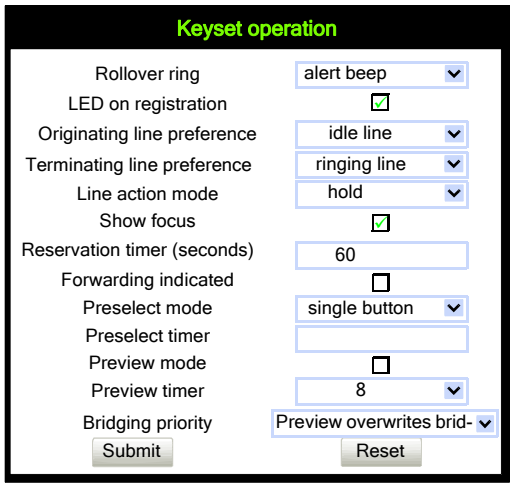
When bridging shall be used, it is highly recommended to configure the phone for a system based conference (see Section 3.7.9, “System Based Conference”). This enables adding more users to a system based conference that has been initiated by bridging.

**Data required**

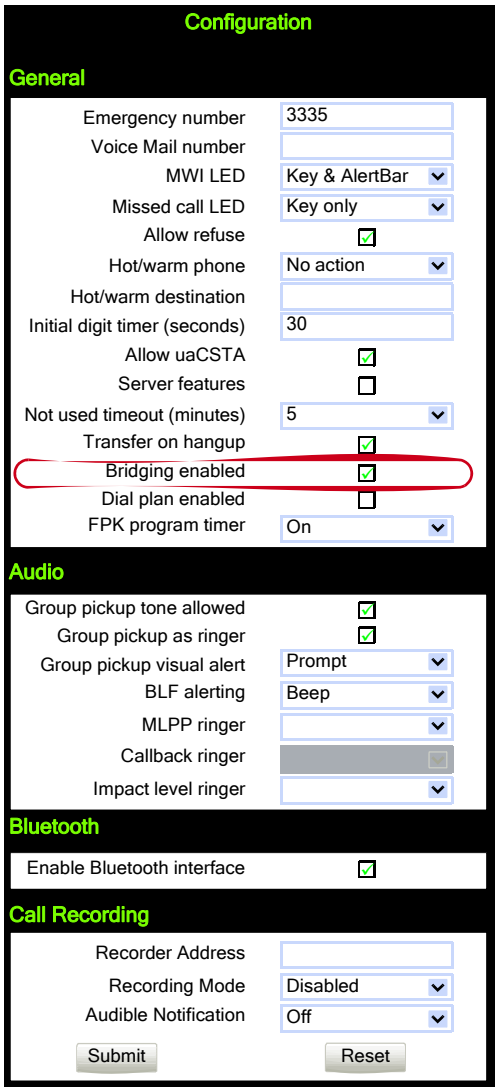
- **Rollover ring**: Determines if a ring tone will signal an incoming call while a call is active.
  Value range: "Standard ring", "No ring", "Alert beep", "Alert ring"
  Default: "Alert beep"
- **LED on registration**: Determines if line LEDs will signal SIP registration.
  Value range: "Yes", "No"
  Default: "Yes"
- **Originating line preference**: Selects the line to be used for outgoing calls.
  Value range: "Idle line", "Primary", "Last", "None"
  Default: "Idle line"
- **Terminating line preference**: Determines which line with an incoming call shall be selected for answering.
  Value range: "Ringing line", "Incoming", "Incoming PLP", "Ringing PLP", "None"
  Default: "Idle line"
- **Line action mode**: Determines the consequence for an established connection when the line key is pressed.
  Value range: "Hold", "Release"
  Default: "Hold"
- **Show focus**: Determines whether the line key LED blinks or is steady when it is in use.
  Value range: "Yes", "No"
  Default: "Yes"
- **Reservation timer**: Sets the period in seconds after which a line reservation is cancelled. If set to 0, the reservation timer is deactivated.
  Default: 60
- **Forward indication**: Activates or deactivates the indication of station forwarding.
  Value range: "Yes", "No"
  Default: "No"
- **Preselect mode**: Determines whether an incoming call is accepted by a single press on the corresponding line key or a double press is needed.
  Value range: "Single button", "Preselection"
  Default: "Single button"
- **Preselect timer**: Sets the timeout in seconds for accepting an incoming call.
- **Bridging enabled** (see Admin > Features > Configuration) : When set to "Yes", the user is allowed to join a call on a shared line. For this purpose, a server based conference is established.

## Administration via WBM

System > Features > Keyset Operation



System > Features > Configuration



### Administration via Local Phone

- Admin
  - System
    - Features
      - Keyset operation
        - **Rollover ring**
        - **LED on registration**
        - **Originating line preference**
        - **Terminating line preference**
        - **Line action mode**
        - **Show focus**
        - **Reservation timer**
        - **Forward indicated**
        - **Preselect mode**
        - **Preselect timer**

### Administration via Local Phone

- Admin
  - System
    - Features
      Configuration
      - General
        - **Bridging enabled**

### 3.11.3 Line Preview

This key enables the preview mode, which allows the user to preview a line before using it.

When preview mode is active, the line keys behave similar to when the keyset configuration is set to preselection for line keys (see Section 3.11.2, “Configure Keyset Operation”). On pressing the line key (not DSS key!), the call activity on the corresponding line is shown. Unlike with a preselected line, there will be no change to the phone’s current line connections. The LED indicates whether line preview is active or not.

The information shown to the user depends on the ring/alert configuration for the line in question. If the line is configured to alert only, the preview will only show the state of the call, not the identity of the call party. If the line is configured to ring, the identity of the call party will be revealed.

The preview mode can be configured as temporary or as permanent. If **System** > **Features** > **Keyset operation** > **Preview mode** is disabled, preview mode will end when the user uses the previewed line, or a new call is started in any other way, or if the focus is changed away from call view. If the parameter is enabled, preview mode remains active until the user cancels it by pressing the key again.

The **Preview timer** parameter determines the timespan during which the line preview will remain on the screen.

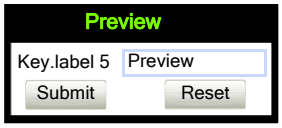
The **Bridging priority** parameter affects the behavior of the line key (see Section 3.11.3.1, “Preview and Preselection”). **Precondition**: Bridging is enabled (see Section 3.11.2, “Configure Keyset Operation”)

**Data required**

- **Preview mode**
  Value range: "Yes", "No"
  Default: "No"
- **Prieview timer**: When Prieview Mode is set, the timer controls preview.
  Value range: 2, 3, 4, 6, 8, 10, 15, 20, 30, 40, 50, 60
  Default: 8
- **Bridging priority**
  Value range: "Prieview overrides bridging", "Bridging overrides preview"
  Default: "Prieview overrides bridging"

## Administration via WBM

System > Features > Program keys > Preview




### 3.11.3.1 Preview and Preselection

Precondition: Bridging is enabled

| Action | Preselect mode | | Preview mode | | Bridging priority | | Result |
|---|---|---|---|---|---|---|---|
| | Single button | Preselection | On (Lock Prev.) | Off (Temp Prev.) | Preview overrides bridging | Bridging overrides preview | |
| Preview key is not pressed (LED off), only the Line key is pressed once or twice | | | | | | | |
| Press busy second. line key 1x | - | ✓ | n.rel. | n.rel. | n.rel. | n.rel. | Line status is displayed (Preselect timer) |
| Press busy second. line key 2x while line-view is displayed | - | ✓ | n.rel. | n.rel. | n.rel. | n.rel. | 1st press: line status<br>2nd press: bridge (conference) |
| Press busy second. line key 1x | ✓ | - | n.rel. | n.rel. | n.rel. | n.rel. | Bridge (conference) |
| Preview key is pressed first (LED on) and the Line key is pressed once or twice | | | | | | | |
| Press busy second. line key 1x | n.rel. | n.rel. | - | ✓ | - | ✓ | Bridge (conference)<br>Preview LED -> off |
| Press busy second. line key 1x | n.rel. | n.rel. | ✓ | - | - | ✓ | Bridge (conference)<br>Preview LED remains on |
| Press busy second. line key 1x | n.rel. | n.rel. | - | ✓ | ✓ | - | Line status is displayed (Preview timer)<br>Preview LED -> off |
| Press busy second. line key 1x | n.rel. | n.rel. | ✓ | - | ✓ | - | Line status is displayed (Preview timer)<br>Preview LED remains on |
| Press busy second. line key 2x while line-view is displayed | n.rel. | n.rel. | - | ✓ | ✓ | - | 1st press: line status<br>2nd press: bridge (conference)<br>Preview LED -> off |
| Press busy second. line key 2x while line-view is displayed | n.rel. | n.rel. | ✓ | - | ✓ | - | 1st press: line status<br>2nd press: bridge (conference)<br>Preview LED remains on |

In case the Preview key is not pressed, only the Preselection mode configuration is relevant:

- if Preselection is selected then the line status is displayed after 1st line press
- if Single button is selected then bridging is invoked (if line busy, bridging enabled)

In case the Preview key is pressed first and then the line key, the Preselection mode configuration is not relevant.

- if Preview mode is activated then the Preview key LED remains on (preview mode must be deactivated manually by pressing the Preview key again).
- if Preview mode is deactivated then the Preview key LED is turned off after preview timer expiry
  - if Bridging priority= Bridging overrides preview then pressing the busy line key invokes bridging
  - if Bridging priority= Preview overrides bridging then pressing the line key displays the line status, however pressing the line key twice bridging will be invoked.

## 3.11.4 Immediate Ring

Enables or disables the preset delay for all line keys. This feature only applies to keyset lines.

The label displayed to the left of the key is defined in **Key label <key number>**.

### Administration via WBM

System > Features > Program keys > Immediate ring

## 3.11.5 Direct Station Select (DSS)

This feature is available only on OpenStage 15/40/60/80, and requires OpenScape Voice.

This feature can be enabled or disabled under System > Features > Feature access (see Section 3.6, “Feature Access”).

A DSS key is a special variant of a line key. It enables a direct connection to a target phone, allowing the user to pick up or forward a call alerting the DSS target and make/complete a call to the DSS target.

### 3.11.5.1 General DSS Settings

These parameters define the behaviour of all DSS keys.

Generally, it is advisable to restrict the user's possibilities to modify line keys, including DSS keys. This can be achieved solely by the DLS. For further instructions, see the DLS Administration Guide.

If the user picks up an incoming call for the DSS target by pressing the associated DSS key, the call is forwarded to the user's primary line. Thereafter, the user's phone rings, and the user can accept the call.

To enable the immediate answering of a call via the DSS key, **Allow auto-answer** in the user menu must be activated. The complete path on the WBM is:
User Pages > Configuration > Incoming calls > CTI calls > Allow auto-answer.

The value of **Call pickup detect timer (seconds)** determines the time interval in which the deflected call is expected at the primary line. When the call arrives whithin this interval, it is given special priority and handling. If a second call arrives on the primary line during this interval, it will be rejected. If a second call arrives outside the interval, it will be treated just like any other incoming call. The default is 3.

If **Deflecting call enabled** is checked, the user can forward an alerting call to the DSS target by pressing the DSS key. The default is "No".

This parameter is configured under System > Features > Feature access (see Section 3.6, “Feature Access”).

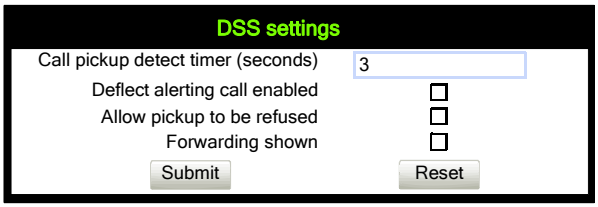
If **Allow pickup to be refused** is checked, the user is enabled to reject a call alerting on the line associated with the DSS key. The default is "No".

This parameter is configured under System > Features > Feature access (see Section 3.6, “Feature Access”).

The DSS key can be configured to indicate the call forwarding state of the number represented by the DSS key. This feature is activated when **Forwarding shown** is enabled.

### Administration via WBM

System > Features > DSS Settings




### Administration via Local Phone

```
└--- Admin
     └--- System
          └--- Features
               └--- DSS operation
                    ├--- Deflect to DSS
                    ├--- Refuse DSS pickup
                    └--- Forwarding shown
```

```
└--- Admin
     └--- System
          └--- Features
               └--- Configuration
                    └--- General
                         └--- DSS Pickup timer
```

### 3.11.5.2 Settings for a DSS key

The **Key label <n>** parameter provides the DSS key with a label that is displayed on the graphic display on an OpenStage 40/60/80 phone. The label is also user configurable.

**Address** contains the call number of the line associated with the DSS key.

The **Realm** parameter stores the SIP Realm of the line associated with the DSS key.

**User Identifier** gives the SIP user ID of the line associated with the DSS key.

**Password** provides the password corresponding to the SIP user ID.

The **Outgoing calls** parameter determines the behaviour of a call over the DSS line at the target phone. If set to "Direct", any forwarding and Do not Disturb settings on the target phone will be overridden, so that a call will always alert. If set to Line type is set to "Normal", this is not the case, and the call will be treated like a regular call.

**Action on calls** defines the handling of an active call when pressing the DSS key. If set to "Consult", the user has an option to start a consultation with the DSS target. If set to "Transfer", the user can only transfer the call to the DSS target. If "No action" is selected, pressing the DSS key will have no effect.

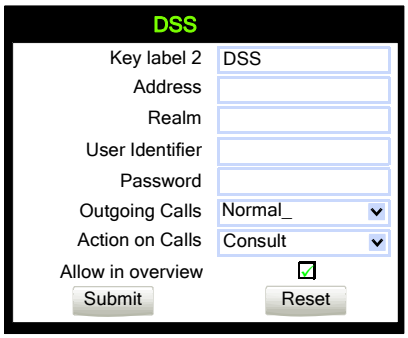
When **Allow in Overview** is set to "Yes", the line corresponding to the DSS key will be visible in the line overview on the phone's display.

### Data required

- **Key label <key number>**: Label to be displayed on the display.
  Default: "DSS"
- **Address**: SIP Address of Record of the destination that is assigned to the DSS key.
- **Realm**: SIP Realm of the DSS destination.
- **User ID**: SIP user ID of the DSS destination.
- **Password**: Password corresponding to the SIP user ID.
- **Outgoing calls**: Determines whether forwarding and DND at the target phone will be overridden on a DSS call.
  Value range: "Normal", "Direct"
  Default: "Normal"
- **Action on calls**: Handling of an active call when pressing the DSS key. "Consult": the user can start a consultation with the DSS target; "Transfer": the user can transfer the call to the DSS target.
  Value range: "Consult", "Transfer", "No action"
  Default: "Consult"
- **Allow in Overview**: Determines whether the line appears in the phone's line overview.
  Value range: "Yes", "No"
  Default: "Yes"

### Administration via WBM

System > Features > Program keys > [edit]



### 3.11.6 Distinctive Ringers per Keyset Lines

For implicit mapping of line ringer names following format is to be used:

"Line-<DN of line>-Reserved"

Thus for a line with DN=1234 the mapped distinctive ringer name is "Line-1234-Reserved". (The name is case-sensitive, mind the uppercase L and R in name.)

The name needs to be manually constructed and configured by Admin as a new ringer name and each such name should be manually checked as being unique in the table.

When using 'Distinctive Ringers per Keyset Lines', it is not allowed to define 'bellcore_dr1', 'bellcore_dr2', and 'bellcore_dr3' in the same distinctive ringer table. Otherwise these settings will be used because of higher priority in SIP-INVITE header. MLPP and Lowel Impact Level calls are also with higher priority.

The "User>Configuration>Keyset>Lines" form has the 'Destination Number' of the line being configured and this can be used to map directly to distinctive ringer names in the "Admin>Ringer setting" form. If a distinctive ringer with a matching name has not been configured into the table then the Ringer related items Ringer, Ringer tone melody, and Ringer sequence in the "User>Configuration>Keyset>Lines" form will be absent. If a matching distinctive ringer name is found then the "Ringer" items are editable with the initially shown value being the same as the value in the "Admin>Ringer setting" form. Changes made to the "Ringer" values by the User will also change the matching distinctive ringer values in "Admin>Ringer setting".

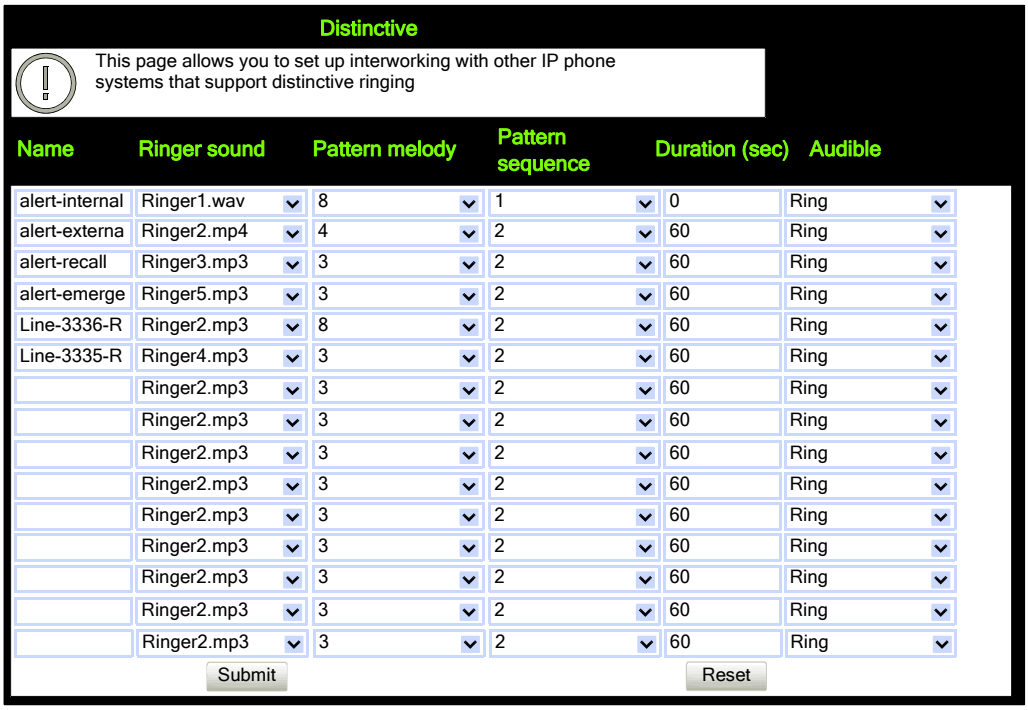
Destinctive Ringers are not applicable for DSS Keys.

#### Data required

- **Name**: Destinctive ringer name .
  Value Range: "Line-<Destination Number of line>-Reserved"
- **Ringer sound**: Specifies whether pattern, i. e. melody, or a specific sound file is used as ringer.
  Default: 'Pattern'
- **Pattern melody**: Determines the melody pattern if **Ringer sound** is set to 'Pattern'.
  Value Range: 1,...,8
- **Pattern sequence**: Determines the length and repetitions of pattern.
  Value Range: "1":1 sec ON, 4 sec OFF,
  "2": 1 sec ON, 2 sec OFF
  "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF
  Default: "1"

## Administration via WBM

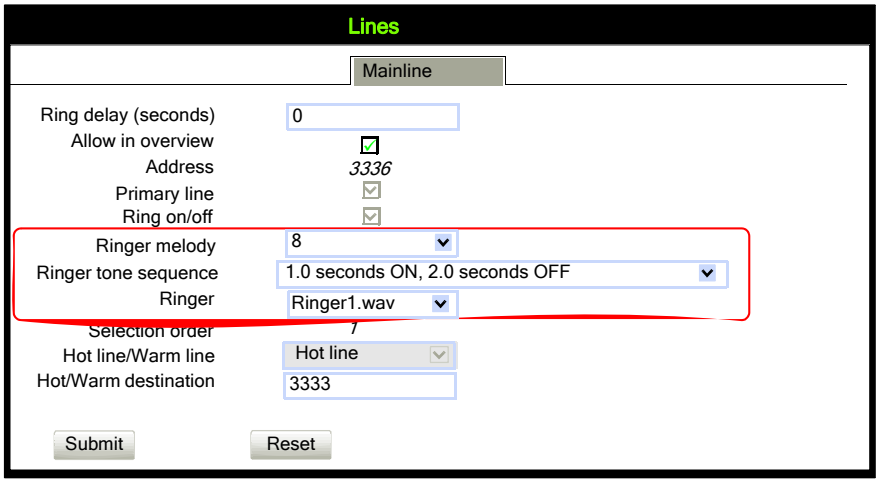
Admin > Ringer setting > Distinctive


Distinctive
This page allows you to set up interworking with other IP phone systems that support distinctive ringing
Name
Ringer sound
Pattern melody
Pattern sequence
Duration (sec)
Audible
alert-internal Ringer1.wav 8 1 0 Ring
alert-externa Ringer2.mp4 4 2 60 Ring
alert-recall Ringer3.mp3 3 2 60 Ring
alert-emerge Ringer5.mp3 3 2 60 Ring
Line-3336-R Ringer2.mp3 8 2 60 Ring
Line-3335-R Ringer4.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Ringer2.mp3 3 2 60 Ring
Submit
Reset

### Administration via Local Phone

- Admin
  - Ringer setting
    - **Distinctive**
      - **<1 .... 15>**
        - **Name**
        - **Ringer sound** (= Ringer in UserMenu)
        - **Pattern melody** (= Ringer melody in UserMenu)
        - **Pattern sequence** (= Ringer tone sequence in User Menu)
        - **Duration**
        - **Audible**

### User menu > Configuration > Keyset > Lines




### Administration via Local Phone

The configuration of a line via Local phone is only possible when the line key has been created via WBM or DLS before by administrator.

- User Menu
  - Configuration
    - Keyset
      - Lines <xx>
        - **Ringer file**(= Ringer sound in Admin Menu)
        - **Ringer melody** (= Pattern melody in Admin Menu)
        - **Ringer sequence** (= Pattern sequence in Admin Menu)

## 3.12 Key Modules

A key module provides 18 (OS 15) or 12 (OS 40/60/80) additional free programmable keys. Key modules are available for OpenStage 15/40/60/80 phones. The key module for the OpenStage 15 phone provides 18 programmable keys. A maximum of 2 key modules can be connected to one phone.

The following table shows which key modules can be connected to the particular phone types.

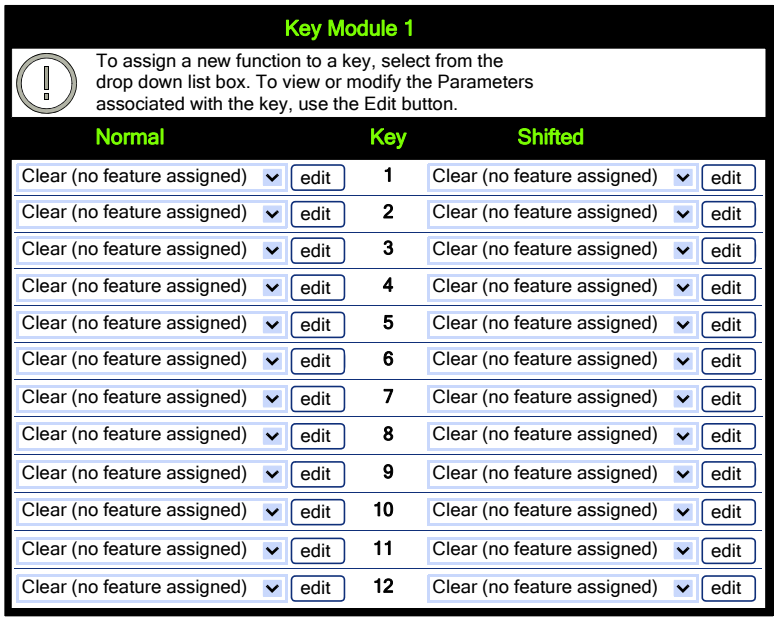
| Phone Type | OpenStage Key Module 15 | OpenStage Key Module |
|---|---|---|
| OpenStage 15 | 1 | - |
| OpenStage 40 | 1 | 2 |
| OpenStage 60/80 | - | 2 |

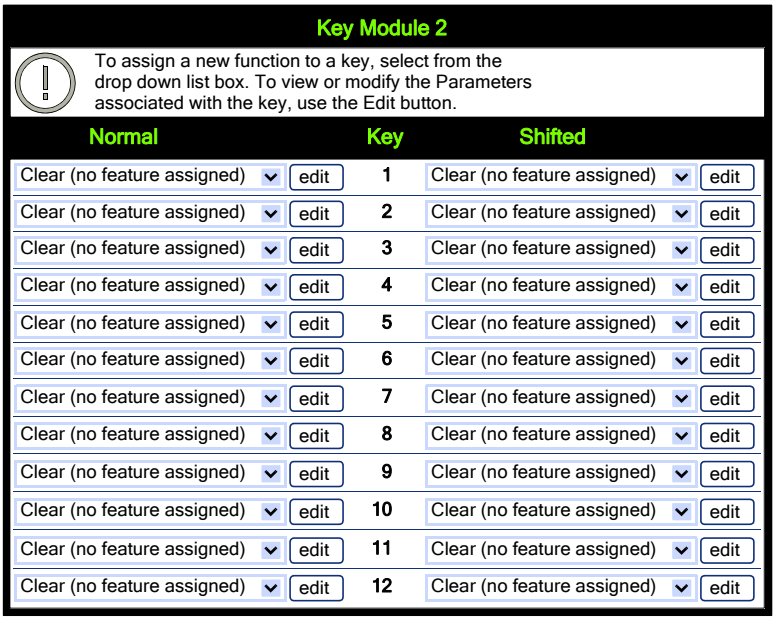
Please note that OpenStage Key Modules (self-labeling) and OpenStage Key Module 15 (paper label) can not be combined. For key labeling, a special tool is available; please refer to: http://wiki.siemens-enterprise.com/index.php/Key_Labelling_Tool .

The configuration of a key on the key module is exactly the same as the configuration of a phone key.

### Administration via WBM

System > Features > Key module 1/2




Key Module 2
To assign a new function to a key, select from the drop down list box. To view or modify the Parameters associated with the key, use the Edit button.
Normal
Key
Shifted
Clear (no feature assigned)
edit
1
2
3
4
5
6
7
8
9
10
11
12

## 3.13 Dialing

### 3.13.1 Canonical Dialing Configuration

Call numbers taken from a directory application, LDAP for instance, are mostly expressed in canonical format. Moreover, call numbers entered into the local phonebook are automatically converted and stored in canonical format, thereby adding "+", **Local country code**, **Local national code**, and **Local enterprise number** as prefixes. If, for instance, the user enters the extension "1234", the local country code is "49", the local national code is "89", and the local enterprise number is "722", the resulting number in canonical format is "+49897221234".

For generating an appropiate dial string, a conversion from canonical format to a different format may be required. The following parameters determine the local settings of the phone, like **Local country code** or **Local national code**, and define rules for converting from canonical format to the format required by the PBX.

To enable the number conversion, all parameters not marked as optional must be provided, and the canonical dial lookup settings must be configured (see Section 3.13.2, “Canonical Dial Lookup”).

**Data required**

- **Local country code**: E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom. Maximum length: 5
- **National prefix digit**: Prefix for national connections, e.g. "0" in Germany and United Kingdom.
  Maximum length: 5
- **Local national code**: Local area code or city code, e.g. "89" for Munich, "20" for London. Maximum length: 6
- **Minimal local number length**: Minimum number of digits in a local PSTN number, e.g. 3335333 = 7 digits.
- **Local enterprise number**: Number of the company/PBX wherein the phone is residing. Maximum length: 10 (Optional)
- **PSTN access code**: Access code used for dialing out from a PBX to a PSTN. Maximum length: 10 (Optional)
- **International access code**: International prefix used to dial to another country, e.g. "00" in Germany and United Kingdom. Maximum length: 5
- **Operator codes**: List of extension numbers for a connection to the operator. The numbers entered here are not converted to canonical format. Maximum length: 50 (Optional)
- **Emergency number**: List of emergency numbers to be used for the phone. If there are more than one numbers, they must be separated by commas. The numbers entered here are not converted to canonical format. Maximum length: 50 (Optional)

These emergency numbers can also be dialed when the phone is locked, in line with the emergency number configured in **Features** > **Configuration** (see Section 3.5.2, “Emergency and Voice Mail”).

- **Initial extension digits** / **Initial digits**: List of initial digits of all possible extensions in the local enterprise network. When a call number could not be matched as a public network number, the phone checks if it is part of the local enterprise network. This is done by comparing the first digit of the call number to the value(s) given here. If it matches, the call number is recognized as a local enterprise number and processed accordingly.
  If, for instance, the extensions 3000-5999 are configured in Phone Administration, each number will start with 3, 4, or 5. Therefore, the digits to be entered are 3, 4, 5.
- **Internal numbers**

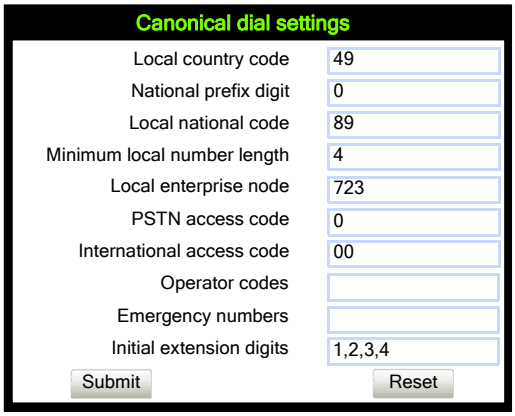
To enable the phone to discern internal numbers from external numbers, it is crucial that a canonical lookup table is provided (Section 3.13.2, “Canonical Dial Lookup”).

  - "Local enterprise form": Default value. Any extension number is dialled in its simplest form. For an extension on the local enterprise node, the node ID is omitted. If the extension is on a different enterprise node, then the appropriate node ID is prefixed to the extension number. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  - "Always add node": Numbers that correspond to an enterprise node extension are always prefixed with the node ID, even those on the local node. Numbers that do not correspond to an enterprise node extension are treated as external numbers.
  - "Use external numbers": All numbers are dialled using the external number form.
- **External numbers**
  - "Local public form": Default value. All external numbers are dialled in their simplest form. Thus a number in the local public network region does not have the region code prefix. Numbers in the same country but not in the local region are dialled as national numbers. Numbers for a different country are dialled using the international format.
  - "National public form": All numbers within the current country are dialled as national numbers, thus even local numbers will have a region code prefix (as dialling from a mobile). Numbers for a different country are dialled using the international format.
  - "International form": All numbers are dialled using their full international number format.
- **External access code**
  - "Not required": The access code to allow a public network number to be dialled is not required.
  - "For external numbers": Default value. All public network numbers will be prefixed with the access code that allows a number a call to be routed outside the enterprise network. However, international numbers that use the + prefix will not be given access code.
- **International gateway code**:

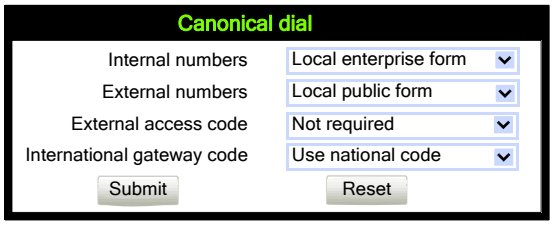
- "Use national code": Default value. All international formatted numbers will be dialled explicitly by using the access code for the international gateway to replace the "+" prefix.
- "Leave as +": All international formatted numbers will be prefixed with "+".

## Administration via WBM

Local functions > Locality > Canonical dial settings




Local functions > Locality > Canonical dial



### Administration via Local Phone

- Admin
  - Local Functions
    - Locality
      - Canonical dial settings
        - **Local country code**
        - **National prefix digit**
        - **Local national code**
        - **Minimum local number length**
        - **Local enterprise node**
        - **PSTN access code**
        - **International code**
        - **Operator code**
        - **Emergency number**
        - **Initial digits**

- Admin
  - Local Functions
    - Locality
      - Canonical dial
        - **Internal numbers**
        - **External numbers**
        - **External access**
        - **International access**

## 3.13.2 Canonical Dial Lookup

The parameters given here are important for establishing outgoing calls and for recognizing incoming calls.

In the local phonebook, and, mostly, in LDAP directories, numbers are stored in canonical format. In order to generate an appropriate dial string according to the settings in **Internal numbers** and **External numbers** (-> Section 3.13.1), internal numbers must be discerned from external numbers. The canonical lookup table provides patterns which allow for operation.

Furthermore, these patterns enable the phone to identify callers from different local or international telephone networks by looking up the caller's number in the phonebook. As incoming numbers are not always in canonical format, their composition must be analyzed first. For this purpose, an incoming number is matched against one or more patterns consisting of country codes, national codes, and enterprise nodes. Then, the result of this operation is matched against the entries in the local phonebook.

To make sure that canonical dial lookup works properly, at least the following parameters of the phone must be provided:

- **Local country code** (-> Section 3.13.1)
- **Local area code** (-> Section 3.13.1)
- **Local enterprise code** (-> Section 3.13.1)

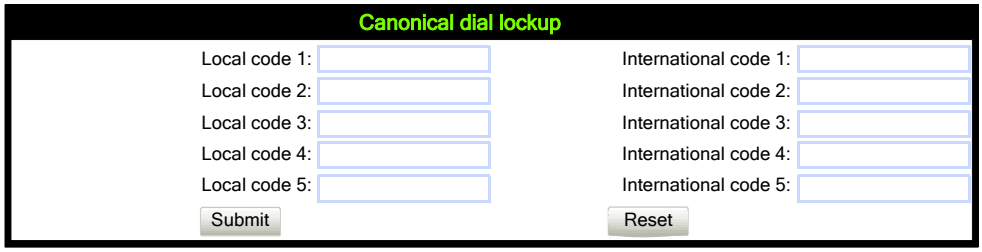
Up to 5 patterns can be defined. The **Local code 1 ... 5** parameters define up to 5 different local enterprise nodes, whilst **International code 1... 5** define up to 5 international codes, that is, fully qualified E.164 call numbers for use in a PSTN.

### Data required

- **Local code 1 ... 5**: Local enterprise code for the node/PBX the phone is connected to. Example: "722" for Siemens Munich.
- **International code 1 ... 5**: Sequence of "+", local country code, local area code, and local enterprise node corresponding to to one or more phonebook entries. Example: "+4989722" for Siemens Munich.

### Administration via WBM

Locality > Canonical dial lookup



### Administration via Local Phone

- Admin
  - Local Functions
    - Locality
      - Canonical Dial Lookup
        - **Local code 1**
        - **International code 1**
        - **Local code 2**
        - **International code 2**
        - **Local code 3**
        - **International code 3**
        - **Local code 4**
        - **International code 4**
        - **Local code 5**
        - **International code 5**

## 3.13.3 Phone location

This parameter specifies if phone location information are included in appropriate SIP messages or not included in any SIP messages but such information are allowed to be configured.

### Data required

- **Phone location**: .
  Value range: "Signalled", "Not signalled"
  Default: "Signalled"

### Administration via WBM

Locality > Phone Location

### Administration via Local Phone

```
└--- Admin
    └--- Local Functions
        └--- Locality
            └--- Phone location
                └--- Phone location
```

## 3.13.4 Dial Plan

OpenStage phones may optionally use a dial plan residing on the phone. By means of the dial plan, the phone can infer from the digits entered by the user that a complete call number has been entered, or that a particular prefix has been entered. Thus, the dialing process can start without the need to confirm after the last digit has been entered, without delay or with a configurable delay. The standard timer, which is found on the WBM under User menu > Configuration > Outgoing calls > Autodial delay (seconds), is overridden if a dial plan rule is matched.

A dial plan consists of rules defining patterns, timeouts and actions to be performed when a pattern is matched and/or a timeout has expired. The phone can store one dialplan, which can contain up to 48 different rules.

It is very important that the phone's dial plan does not interfere with the dial plan in the SIP server, PBX, or public network.

The dial plan can be created and uploaded to the phone using the DLS (please refer to the Deployment Service Administration Manual). The DLS can also export and import dial plans in .csv format. For details about the composition of a dial plan, please refer to Section 5.5, "Dial Plan".

The current dial plan, along with its status (enabled/disabled) and error status can be displayed on the WBM via Diagnostics > Fault trace configuration > Download dial plan file.

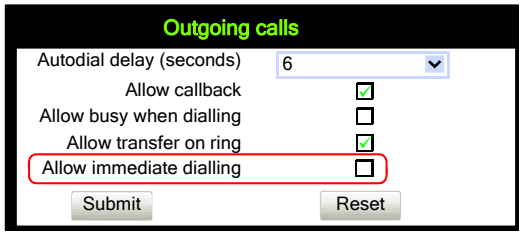
With software version V2R2, the **Dial plan ID** and the **Dial plan status** is displayed in the local menu.

To make use of the dial plan facility, the following requirements must be met:

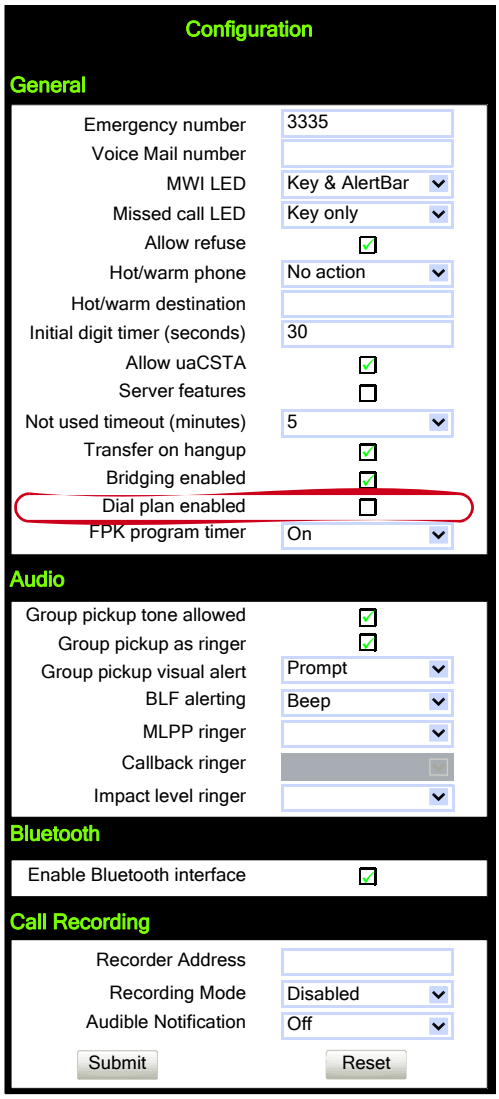
- A correct dial plan is loaded to the phone.
- In the user menu, **Allow immediate dialing** is enabled.
- **Dial plan enabled** is checked.

### Administration via WBM (User menu)

User > Configuration > Outgoing calls > Allow immediate dialing



System > Features > Configuration > Dial plan enabled



### Administration via Local Phone

- User
  - Configuration
    - Outgoing calls
      - **Immediate dialing**

- Admin
  - System
    - Features
      - Configuration
        - General
          - **Dial plan**

- Admin
  - General Information
    - **Dial plan ID**
    - **Dial plan status**

## 3.14 Ringer Setting

### 3.14.1 Distinctive

The SIP server may provide information indicating a specific type of call within an incoming call. The phone can use this information to choose a ring tone according to the call type from the "Distinctive ringer table".

The relevant information is carried as a string in the SIP Alert-Info header. This string is configured in the OpenScape Voice system; please refer to the relevant OpenScape Voice documentation. When the string sent via alert-info matches the string specified in the **Name** parameter, the corresponding ringer is triggered. For instance, the OpenScape Voice system may send the string `Bellcore-dr1` to indicate that a call is from within the same business group, and the **Name** parameter is set to "Bellcore-dr1". To select a specific ring tone for calls from the same business group, the other parameters corresponding to that **Name** must be set accordingly.

The **Ringer sound** parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

**Pattern melody** selects the melody pattern that will be used if **Ringer sound** is set to "Pattern".

**Pattern sequence** determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF
- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF

The **Duration** parameter determines how long the phone will ring on an incoming call. The range is 0-300 sec.

With the **Audible** parameter, the ringer can be muted. In this case, an incoming call will be indicated only visually.

**Special Ringers** can be configured for the following call types:

- Internal
- External
- Recall
- Emergency
- Special1
- Special2
- Special3

To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer sound, Pattern Melody, and Pattern sequence.

Abstract names used for **Special Ringers**:

•"Bellcore-dr1" - normal (internal) alerting or ring-back;

•"Bellcore-dr2" - external alerting or ring-back;

•"Bellcore-dr3" - recall alerting or ring-back (e.g., following transfer).

•"alert-internal" - normal (internal) alerting or ring-back;

•"alert-external" - external alerting or ring-back;

•"alert-recall" - recall alerting or ring-back (e.g., following transfer)

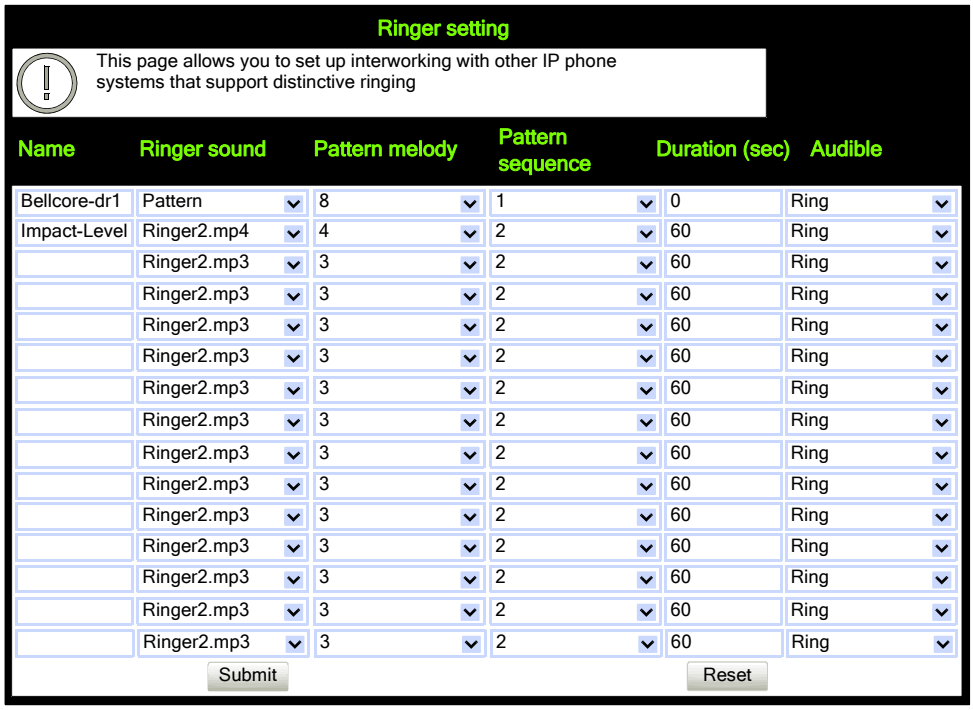
•"alert-emergency" - emergency alerting or ring-back.

•"Line-<DN of Line>-Reserved" - distinctive alerting for a line with number <DN of Line>

Once made available (by the administrator) to the user, the **Special Ringers** for the call types listed can be selected and configured via the **User** menu as shown in *Section 3.14.3, “Special Ringers”*.

**Administration via WBM**

Admin > Ringer setting > Distinctive




### Administration via Local Phone

- Admin
  - Ringer setting
    - **Distinctive**
      - **<1 .... 15>**
        - **Name**
        - **Ringer sound**
        - **Pattern melody**
        - **Pattern sequence**
        - **Duration**
        - **Audible**

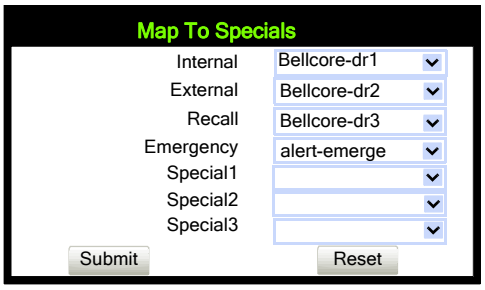
## 3.14.2 Map to Specials

The "Mapping table" is not accessible by local menu, WBM, or DLS but is predefined with Ringer name defaults. Only the special ringers for the default types will be shown in the local menu and WBM. If a default Ringer name is not configured in the "Distinctive ringer table" then the mapped entry in the "Special ringer table" will be greyed and read-only.

The "Mapping table" has been configured to identify the distinctive ringer names as a special ringer type and the User has access to configure a different audio file or pattern for this distinctive ringer via their "Special ringer table". Any change made by the User to this special ringer will be reflected in the "Distinctive ringer table" and any change made by Admin in the "Distinctive ringer table" will be reflected in the "Special ringer table".

### Administration via WBM

Admin > Ringer setting > Map To Specials




## 3.14.3 Special Ringers

**Special Ringers** can be configured via the **User** menu for the following call types:

- Internal
- External
- Recall
- Emergency
- Special1
- Special2
- Special3

### Administration via WBM (User menu)

User > Audio > Special ringers

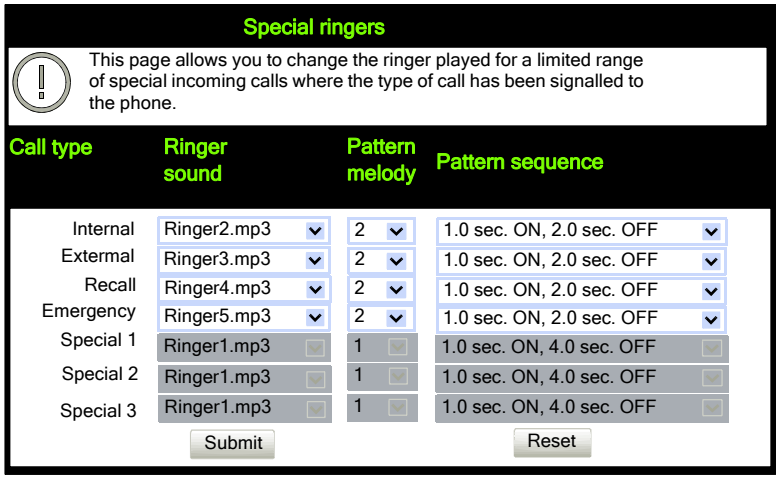
The **Special ringers** dialog allows the user to change the ring tones for the special call types listed below, provided that the call type is signaled to the phone.

To make the special ringers available and configurable to the user, the administrator needs to map the call types to specific ringers via the **Ringer setting** mapping table in **Admin > Ringer setting > Distinctive**. Each call type can be mapped to a specific Ringer sound, Pattern melody, and Pattern sequence.

### Special Ringer Call Types

- Internal
- External
- Recall
- Emergency
- Special1
- Special2

- Special3




### Administration via Local Phone

└── User
  └── Audio
    └── <**Special Ringers**>
      ├── **Internal**
      ├── **External**
      ├── **Recall**
      ├── **Emergency**
      ├── **Special 1**
      ├── **Special 2**
      └── **Special 3**

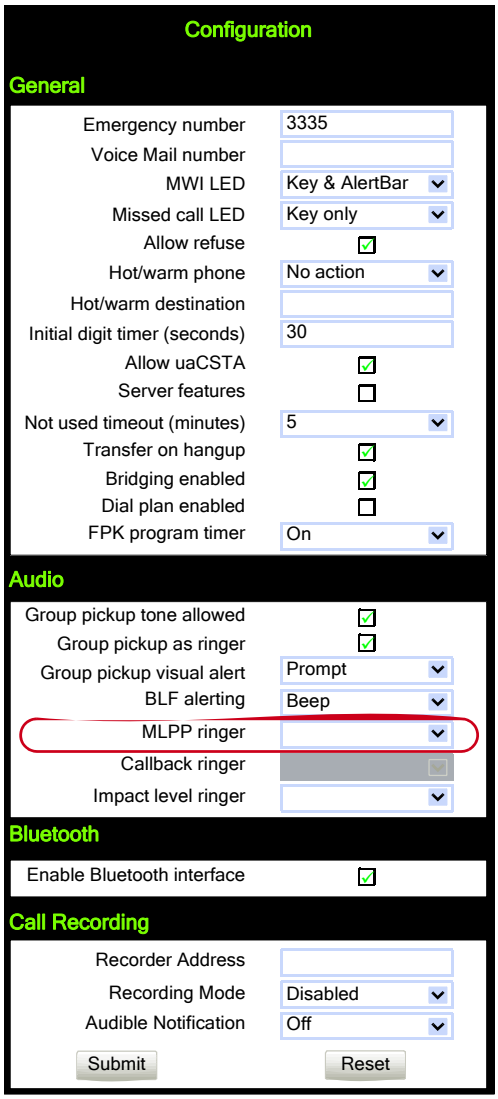
For each call type, the following parameters can be configured:

The **Ringer sound** parameter determines whether a pattern, i. e. melody, or a specific sound file shall be used as ringer.

**Pattern melody** selects the melody pattern that will be used if **Ringer sound** is set to "Pattern".

**Pattern sequence** determines the length for the melody pattern, and the interval between the repetitions of the pattern. There are 3 variants:

- "1": 1 sec ON, 4 sec OFF
- "2": 1 sec ON, 2 sec OFF
- "3": 0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF


Configuration
General
Emergency number
3335
Voice Mail number
MWI LED
Key & AlertBar
Missed call LED
Key only
Allow refuse
Hot/warm phone
No action
Hot/warm destination
Initial digit timer (seconds)
30
Allow uaCSTA
Server features
Not used timeout (minutes)
5
Transfer on hangup
Bridging enabled
Dial plan enabled
FPK program timer
On
Audio
Group pickup tone allowed
Group pickup as ringer
Group pickup visual alert
Prompt
BLF alerting
Beep
MLPP ringer
Callback ringer
Impact level ringer
Bluetooth
Enable Bluetooth interface
Call Recording
Recorder Address
Recording Mode
Disabled
Audible Notification
Off
Submit
Reset

## 3.15 Mobility

The Mobility feature requires the OpenScape Deployment Service (DLS). If the phone is mobility enabled by the DLS, a mobile user can log on to the phone and thereby have his own user settings transferred to the phone. These user data are stored in the DLS database and include, for instance, SIP registration settings, dialing properties, key layouts, as well as the user's phonebook.

If the mobile user changes some settings, the changed data is sent to the DLS server. This ensures that his user profile is updated if necessary.

If **Unauthorized Logoff Trap** is set to "Yes", a message is sent to the SNMP server if an unauthorized attempt is made to log off the mobile user.

**Logoff Trap Delay** defines the time span in seconds between the unauthorized logoff attempt and the trap message to the SNMP server.

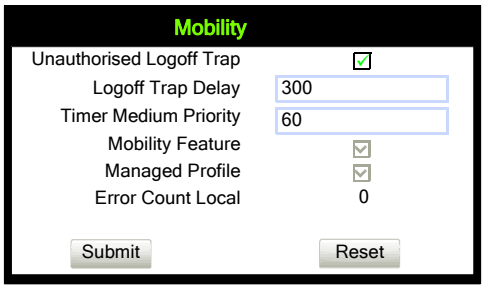
**Timer Medium Priority** determines the time span in seconds between a change of user data in the phone and the transfer of the changes to the DLS server.

The **Mobility Feature** parameter indicates whether the mobility feature is enabled by the DLS or not.

**Data required**

- **Unauthorized Logoff Trap**: An SNMP trap is sent on an unauthorized logoff attempt.
  Value range: "Yes", "No"
  Default: "No"
- **Logoff Trap Delay**: Time span in seconds between the unauthorized logoff attempt and the SNMP trap.
  Default: 300
- **Timer Medium Priority**: Time span in seconds between a data change in the phone and its transfer to the DLS server.
  Default: 60
- **Mobility feature**: Indicates whether the mobility feature is enabled.
- **Managed Profile**: Display only field.
- **Error Count Local**: Display only field.

## Administration via WBM




## Administration via Local Phone

- Admin
  - Mobility
    - **Unauthorized Logoff Trap**
    - **Logoff Trap Delay**
    - **Timer Medium Priority**
    - **Mobility Feature**
    - **Managed Profile**
    - **Error Count Local**

## 3.16 Transferring Phone Software, Application, and Media Files

New software images, hold music, picture clips for phonebook entries, LDAP templates, company logos, screensaver images, and ring tones can be uploaded to the phone via DLS (Deployment Service) or WBM (Web Based Management).

If an incorrect software image is being attempted to be loaded onto the phone, the phone will reject the request and return to normal operation without reboot. As part of this security mechanism, new software binds are identified by a "Supported Hardware Level" information built into the header.

For all user data, which includes files as well as phonebook content, the following amounts of storage place are available:

- OpenStage 15/20/40: 2,5 MB
- OpenStage 60/80: 8 MB

### 3.16.1 FTP/HTTPS Server

There are no specific requirements regarding the FTP server for transferring files to the OpenStage phone. Any FTP server providing standard functionality will do.

### 3.16.2 Common FTP/HTTPS Settings

For each one of the various file types, e.g. phone software, hold music, and picture clips, specific FTP/HTTPS access data can be defined. If some or all file types have the parameters **Download method**, **Server address**, **Server port**, **Account**, **Username**, **FTP path**, and **HTTPS base URL** in common, they can be specified here. These settings will be used for a specific file type if its **Use defaults** parameter is set to "Yes".

If **Use defaults** is activated for a specific file type, any specific settings for this file type are overridden by the defaults.

Additional log messages are issued for the following scenarios

- Update has been allowed due to override flag being set
- Whole part number is not recognized
- Block 4 of part number is not recognized
- Downloaded software does not have a hardware level included

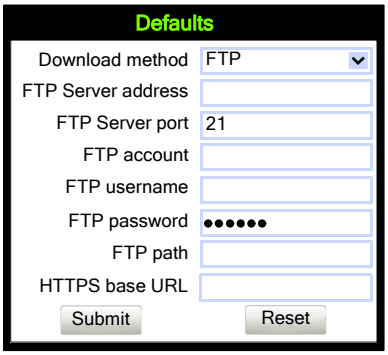
#### Data required

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **FTP Server address**: IP address or hostname of the FTP server in use.

- **FTP Server port**: Port number of the FTP server in use. For HTTPS, port 443 is assumed, unless a different port is specified in the HTTPS base URL.
  Default: 21
- **FTP Account**: Account at the server (if applicable).
- **FTP Username**: User name for accessing the server.
- **FTP Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use. If no port number is specified here, port 443 is used. Only applicable if **Download method** is switched to "HTTPS".

### Administration via WBM

File transfer > Defaults




### Administration via Local Phone

```
└── Admin
    └── File Transfer
        └── Defaults
            ├── Download method
            ├── Server
            ├── Port
            ├── Account
            ├── Username
            ├── Password
            ├── FTP path
            └── HTTPS base URL
```

## 3.16.3 Phone Software

The firmware for the phone can be updated by downloading a new software file to the phone.

If an incorrect software image is being attempted to be loaded onto the phone, the phone will reject the request and return to normal operation without reboot. As part of this security mechanism, new software binds are identified by a "Supported Hardware Level" information built into the header.

Prerequisite: The phone knows its own hardware level (from the part number and/or by a dynamical check of its HW level).

When a new software bind is downloaded to the phone, the following verifcation is performed:

1. If new software bind has hardware level header included (in the bind header):
   Hardware level of new bind is compared with phone's hardware level
   a) If compatible (or if Override is set): Proceed with update
   b) If NOT compatible: Abandon update and return to original application
2. If new software bind does NOT have hardware level header included (in the bind header):
   Software version of new bind is compared with minimum known supported SW level
   a) If compatible (or if Override is set): Proceed with update
   b) If NOT compatible: Abandon update and return to original application

Do not disconnect the phone from the LAN or power unit during software update. An active update process is indicated by blinking LEDs and/or in the display.

### 3.16.3.1 FTP/HTTPS Access Data

If the default FTP/HTTPS Access settings (see Section 3.16.2, "Common FTP/HTTPS Settings") are to be used, **Use defaults** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

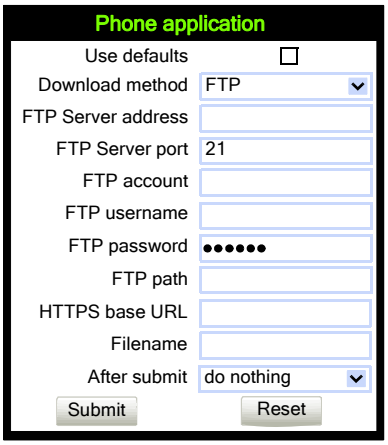
- **Use defaults**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No".
  Default: "No".
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies action after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

## Administration via WBM

File transfer > Phone application




## Administration via Local Phone

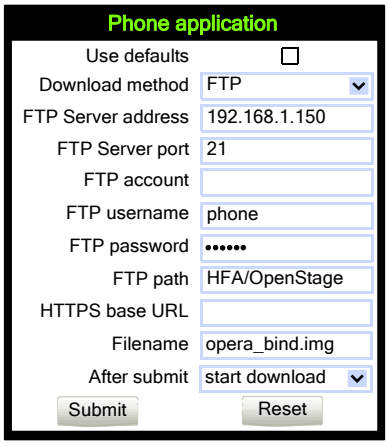
- Admin
  - File Transfer
    - Phone app
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

### 3.16.3.2 Download/Update Phone Software

If applicable, phone software should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu. When the download has been successful, the phone will restart and boot up using the new software.

When Phone Software was upgraded to V3R3 there may be displayed a downgrade protection message.

#### Start Download via WBM




In the **File transfer** > Phone application dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Phone app**.

```
└── Admin
    └── File Transfer
        └── Phone app
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.4 Music on Hold

If enabled by the user, the Music on Hold (MoH) sound file is played when a call is put on hold.

The file size for a Music on Hold file is limited to 1MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

The following formats for Music on Hold are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit
- MIDI format
- MP3 format (OpenStage 60/80 only). A bitrate of 48 kB/sec is recommended.

### 3.16.4.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use Default** smust be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

- **Use defaults**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies action after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

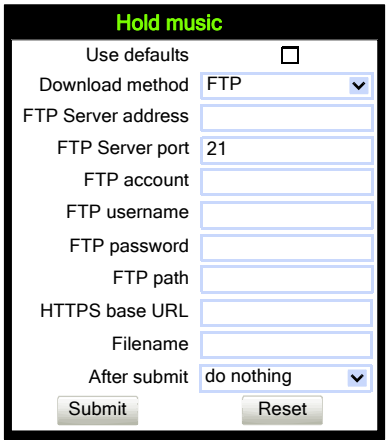
**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.

- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

### Administration via WBM

File transfer > Hold music



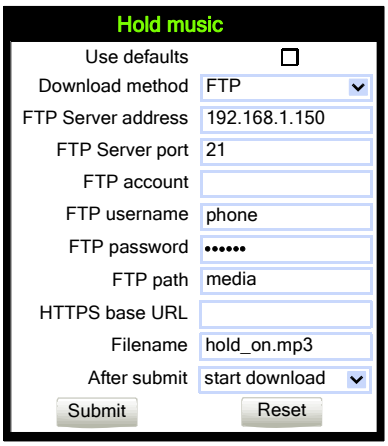

### Administration via Local Phone

```
└── Admin
    └── File Transfer
        └── Hold Music
            ├── Use default
            ├── Download method
            ├── Server
            ├── Port
            ├── Account
            ├── Username
            ├── Password
            ├── FTP path
            ├── HTTPS base URL
            └── Filename
```

### 3.16.4.2 Download Music on Hold

If applicable, Music on Hold should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

#### Start Download via WBM




In the **File transfer** > **Hold music** dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Hold Music**.

```
└--- Admin
     └--- File Transfer
          └--- Hold Music
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.5 Picture Clips

Picture clips are available only on OpenStage 60/80 phones.

The file size for a picture clip is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

Picture Clips are small images used for displaying a picture of a person that is calling on a line. The supported file formats for picture clips are JPEG and PNG (recommended).

### 3.16.5.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

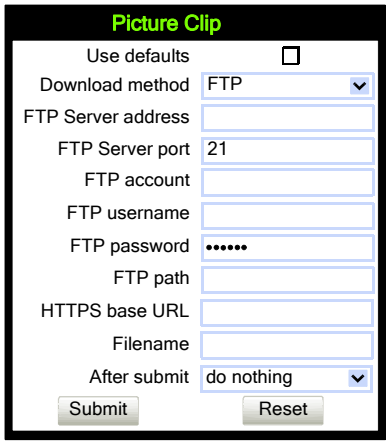
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies action after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

## Administration via WBM

File transfer > Picture clip



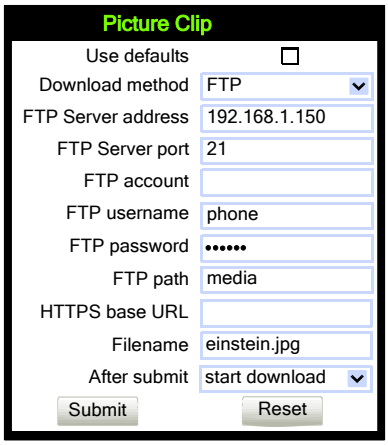

## Administration via Local Phone

- Admin
  - File Transfer
    - Picture Clip
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

### 3.16.5.2 Download Picture Clip

The download can be triggered from the web interface or from the local phone menu.

#### Start Download via WBM




In the **File transfer** > Picture clip dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Picture clip**.

└--- Admin
  └--- File Transfer
    └--- **Picture clip**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.6 LDAP Template

LDAP is available on OpenStage 15/20/40/60/80.

The LDAP template is an ASCII text file that uses an allocation list to assign directory server attributes to input and output fields on an LDAP client. The LDAP template must be modified correctly for successful communication between the directory server and the LDAP client.

The OpenStage phones support LDAPv3.

### 3.16.6.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

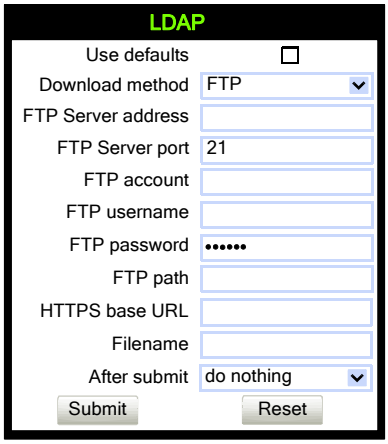
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

## Administration via WBM

File transfer > LDAP




## Administration via Local Phone

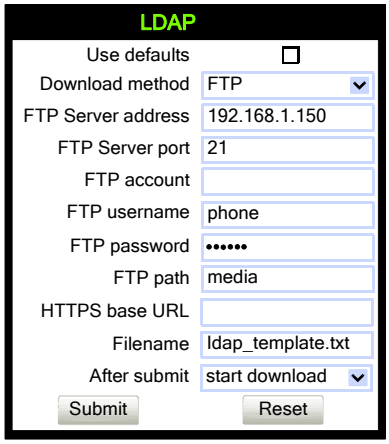
- Admin
  - File Transfer
    - LDAP
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

### 3.16.6.2 Download LDAP Template

If applicable, LDAP templates should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

The OpenStage phone supports LDAPv3.

#### Start Download via WBM




In the **File transfer** > LDAP dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **LDAP**.

└─ Admin
  └─ File Transfer
    └─ **LDAP**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.7 Logo

On OpenStage 40/60/80, a custom background image for the telephony interface can be supplied. In most cases, this will be the company logo.

On OpenStage 40, monochrome bitmap files (BMP) are supported. The ideal size is as follows:

- Width: 144 px
- Height: 32 px

On OpenStage 60/80, the supported file formats are JPEG and PNG. The ideal size values are is as follows:

OpenStage 60:

- Width: 240 px
- Height: 70 px

OpenStage 80:

- Width: 480 px
- Height: 142 px

If the size should deviate from these values, the image will appear skewed.

For guidance on creating a logo file for OpenStage 40/60/80, see Section 5.2, “How to Create Logo Files for OpenStage Phones”.

### 3.16.7.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

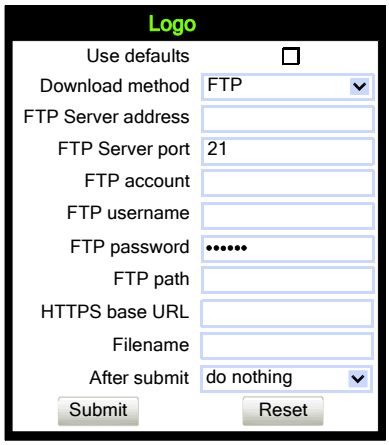
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
- Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

### Data required (if not derived from Defaults)

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

### Administration via WBM

File transfer > Logo



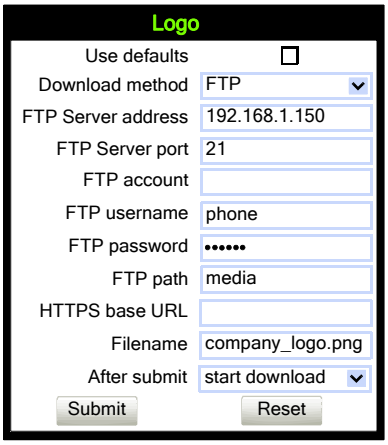

### Administration via Local Phone

```
└── Admin
    └── File Transfer
        └── Logo
            ├── Use default
            ├── Download method
            ├── Server
            ├── Port
            ├── Account
            ├── Username
            ├── Password
            ├── FTP path
            ├── HTTPS base URL
            └── Filename
```

### 3.16.7.2 Download Logo

If applicable, logos should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

#### Start Download via WBM




In the **File transfer** > Logo dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Logo**.

└─ Admin
  └─ File Transfer
    └─ **Logo**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.8 Screensaver

The screensaver is displayed when the phone is in idle mode. It performs a slide show consisting of images which can be uploaded using the web interface.

Screensavers are available only on OpenStage 60/80 phones.

The file size for a screensaver image is limited to 300 KB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone.

For screensaver images, the following specifications are valid:

- Data format: JPG or PNG. JPG is recommended.
- Screen format: 4:3. The images are resized to fit in the screen, so that images with a width/height ratio differing from 4:3 will appear with deviant proportions.
- Resolution: The phone's screen resolution is the best choice for image resolution:
  - OpenStage 60: 320x240
  - OpenStage 80: 640x480

### 3.16.8.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, "Common FTP/HTTPS Settings") are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

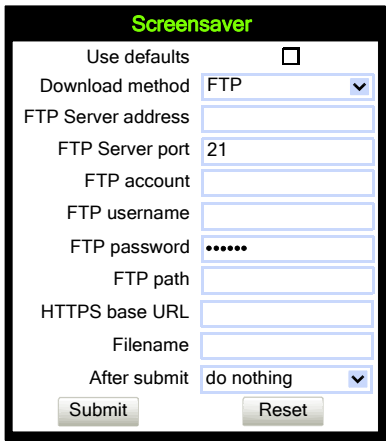
**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.

- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

### Administration via WBM

File transfer > Screensaver



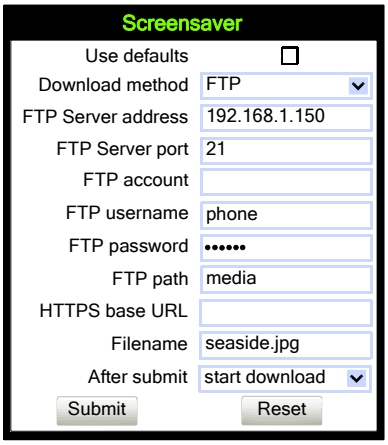

### Administration via Local Phone

```
└── Admin
    └── File Transfer
        └── Screensaver
            ├── Use default
            ├── Download method
            ├── Server
            ├── Port
            ├── Account
            ├── Username
            ├── Password
            ├── FTP path
            ├── HTTPS base URL
            └── Filename
```

### 3.16.8.2 Download Screensaver

If applicable, screensavers should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

#### Start Download via WBM




In the **File transfer** > Screensaver dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Screensaver**.

└── Admin
  └── File Transfer
    └── **Screensaver**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

### 3.16.9 Ringer File

Custom ring tones can be uploaded to the phone.

The file size for a ringer file is limited to 1 MB. If the file is too large or the contents of the file are not valid, the file will not be stored in the phone. This limitation is only enforced on WBM. If a ringer file is downloaded via OpenStage Manager, this restriction does not apply.

The following file formats are supported:

- WAV format. The recommended specifications are:
  - Audio format: PCM
  - Bitrate: 16 kB/sec
  - Sampling rate: 8 kHz
  - Quantization level: 16 bit
- MIDI format.
- MP3 format (OpenStage 60/80 only). The OpenStage 60/80 phones are able to play MP3 files from 32 kbit/s up to 320 kbit/s. As the memory for user data is limited to 8 MB, a constant bitrate of 48 kbit/sec to 112 kbit/s and a length of max. 1 minute is recommended. Although the phone software can play stereo files, mono files are recommended, as the phone has only 1 loudspeaker.
  See the following table for estimated file size (mono files):

| **Length** | **64 kbit/s** | **80 kbit/s** | **96 kbit/s** | **112 kbit/s** |
|---|---|---|---|---|
| 0:15 min | 0,12 MB | 0,15 MB | 0,18 MB | 0,21 MB |
| 0:30 min | 0,23 MB | 0,29 MB | 0,35 MB | 0,41 MB |
| 0:45 min | 0,35 MB | 0,44 MB | 0,53 MB | 0,62 MB |
| 1:00 min | 0,47 MB | 0,59 MB | 0,70 MB | 0,82 MB |

### 3.16.9.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to "Yes", and only the **Filename** must be specified.

**Data required (in any case)**

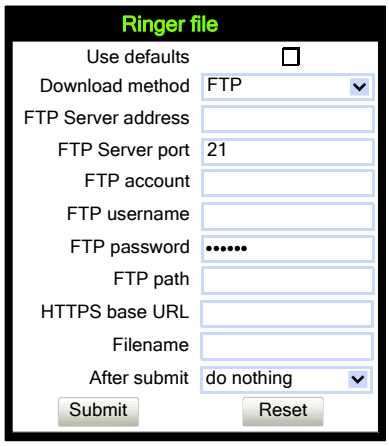
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: "Yes", "No"
  Default: "No"
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies action after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: "FTP", "HTTPS"
  Default: "FTP"
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to "HTTPS".

### Administration via WBM

File transfer > Ringer file



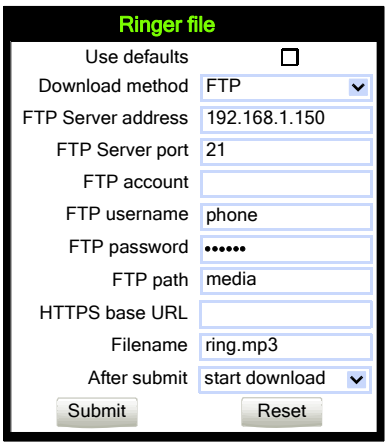

### Administration via Local Phone

- Admin
  - File Transfer
    - Ringer
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

### 3.16.9.2 Download Ringer File

If applicable, ring tone files should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

#### Start Download via WBM




In the File transfer > Ringer dialog, set **After submit** to "start download" and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Ringer**.

```
└--- Admin
     └--- File Transfer
          └--- Ringer
```

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.16.10 Dongle Key

The HPT dongle key is a special file that contains a secret hash number which is required to connect the HPT tool to the phone. This testing tool is used exclusively by the service staff.

### 3.16.10.1 FTP/HTTPS Access Data

If the default FTP/HTTPS access settings (see Section 3.16.2, “Common FTP/HTTPS Settings”) are to be used, **Use default** must be set to „Yes“, and only the **Filename** must be specified.

**Data required (in any case)**

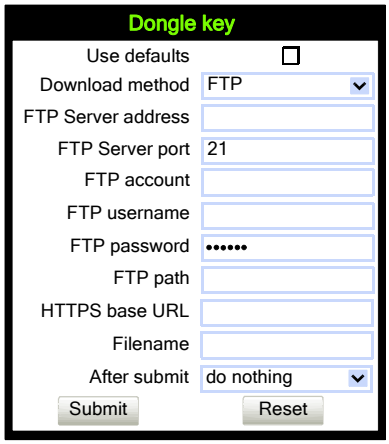
- **Use default**: Specifies whether the default FTP/HTTPS access settings shall be used.
  Value range: „Yes“, „No“
  Default: „No“
- **Filename**: Specifies the file name of the phone software.
- **After submit**: Specifies actions after submit button is pressed.
  Value range: "do nothing", "start download".
  Default: "do nothing".

**Data required (if not derived from Defaults)**

- **Download method**: Selects the protocol to be used.
  Value range: „FTP“, „HTTPS“
  Default: „FTP“
- **Server address**: IP address or hostname of the FTP/HTTPS server in use.
- **Server port**: Port number of the FTP/HTTPS server in use.
  Default: 21
- **Account**: Account at the server (if applicable).
- **Username**: User name for accessing the server.
- **Password**: Password corresponding to the user name.
- **FTP path**: Path of the directory containing the files.
- **HTTPS base URL**: IP address or hostname of the HTTPS server in use; only applicable if **Download method** is switched to „HTTPS“.

## Administration via WBM

**File transfer** > Dongle key



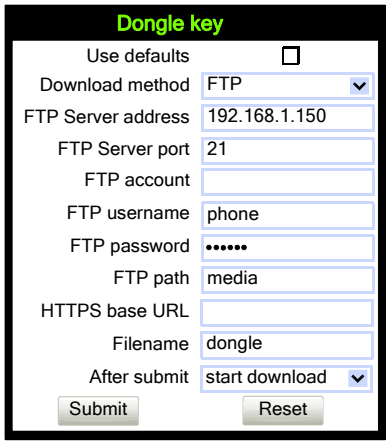

## Administration via Local Phone

- Admin
  - File Transfer
    - Dongle key
      - **Use default**
      - **Download method**
      - **Server**
      - **Port**
      - **Account**
      - **Username**
      - **Password**
      - **FTP path**
      - **HTTPS base URL**
      - **Filename**

### 3.16.10.2 Download Dongle Key File

If applicable, dongle key files should be deployed using the DLS (Deployment Service). Alternatively, the download can be triggered from the web interface or from the Local phone menu.

#### Start Download via WBM




In the **File transfer** > Dongle key dialog, set **After submit** to „start download“ and press the **Submit** button.

#### Start Download via Local Phone

1. In the administration menu, set the focus to **Dongle key**.

└--- Admin
  └--- File Transfer
    └--- **Dongle key**

2. Press the ➔ key. A context menu opens. In the context menu, select **Download**. The download will start immediately.

## 3.17 Corporate Phonebook: Directory Settings

### 3.17.1 LDAP

LDAP is available on OpenStage 15/20/40/60/80 with SIP V3R3.

The Lightweight Directory Access Protocol enables access to a directory server via an LDAP client. Various personal information is stored there, e.g. the name, organization, and contact data of persons working in an organization. When the LDAP client has found a person's data, e. g. by looking up the surname, the user can call this person directly using the displayed number.

The OpenStage phones support LDAPv3.

For connecting the phone's LDAP client to an LDAP server, the required access data must be configured. The parameter **Server address** specifies the IP address of the LDAP server. The parameter **Transport** defines whether the phone has to continue to use an unencrypted TCP connection to the LDAP server, or to use an encrypted TLS connection to a separate LDAPS port on the LDAP server. Depending on the setting of **Transport** the **Secure Port** (for TLS) or the **Server port** (for TCP) are to be defined. If the **Authentication** is not set to "Anonymous", the user must authenticate himself with the server by providing a **User name** and a corresponding **Password**. The user name and password are defined by the administrator. The user name is the string in the LDAP bind request, e. g. "C=GB,O=SIEMENS COMM,OU=COM,L=NTH,CN=BAYLIS MICHAEL". The internal structure will depend on the specific corporate directory.

For a quick guide on setting up LDAP on an OpenStage phone, please refer to Section 5.3, "How to Set Up the Corporate Phonebook (LDAP)".

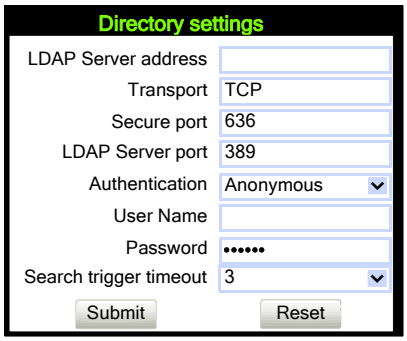
#### Data required

- **Server address**: IP address or hostname of the LDAP server.
- **Transport**: Defines Transport mode, whether LDAP interface uses TCP and is unencrypted, or uses TLS and is encrypted.
  Value range: "TCP", "TLS"
  Default: "TCP"
- **Secure Port**: Defines the port of the appropriate TLS interface on LDAP server when **Transport** is set to TLS.
  Default: "636"

- **Server port**: Port on which the LDAP server is listening for requests, when **Transport** is set to TCP.
  Default: 389
- **Authentication**: Authentication method used for connecting to the LDAP server.
  Value range: "Anonymous", "Simple"
  Default: "Anonymous"
- **User name**: User name used for authentication with the LDAP server in the LDAP bind request.
- **Password**: Password used for authentication with the LDAP server.
- **Search trigger timeout**: Timespan between entering the last character and search string submission to the LDAP server.

### Administration via WBM

Local Functions > Directory settings




### Administration via Local Phone

```
└--- Admin
    └--- Local Functions
        └--- LDAP
            |--- Server address
            |--- Transport
            |--- LDAP secure port
            |--- LDAP server port
            |--- Authenticate
            |--- User name
            |--- Password
            └--- Search trigger (s)
```

## 3.18 Speech

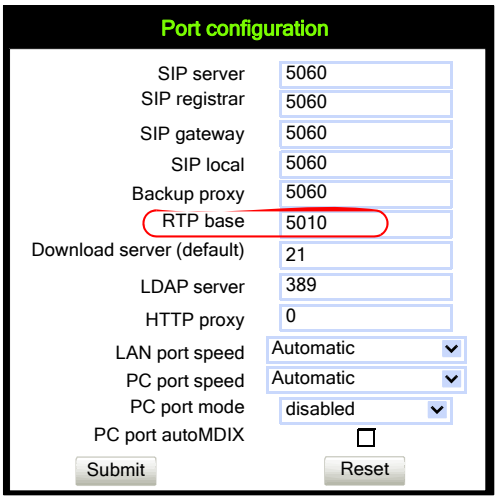
### 3.18.1 RTP Base Port

The port used for RTP is negotiated during the establishment of a SIP connection. The RTP base port number defines the starting point from which the phone will count up when negotiating. The default value is 5010.

The number of the port used for RTCP will be the RTP port number increased by 1.

#### Administration via WBM

Network > Port Configuration




#### Administration via Local Phone

```
└── Admin
    └── Network
        └── Port Configuration
            └── RTP base
```

## 3.18.2 Codec Preferences

If **Silence suppression** is activated, the transmission of data packets is suppressed on no conversation, that is, if the user doesn't speak.

The OpenStage phone provides the codecs **G.711**, **G.722**, and **G.729**. When a SIP connection is established between two endpoints, the phones negotiate the codec to be used. The result of the negotiation is based on the general availability and ranking assigned to each codec. The administrator can allow or disallow a codec as well as assign a ranking number to it.

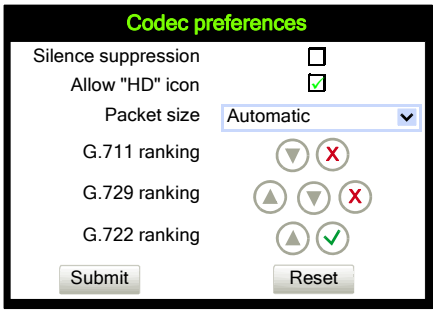
The **Packet size**, i. e. length in milliseconds, of the RTP packets for speech data, can be set to 10ms, 20ms, 30ms, 60ms or to automatic detection.

**Data required**

- **Silence suppression**: Suppression of data transmission on no conversation.
  Value range: "On", "Off"
  Default: "Off"
- **Allow "HD" icon**: If "On" an additional icon is shown when codec G.722 is used.
  Value range: "On", "Off"
  Default: "On"
- **Packet size**: Size of RTP packets in milliseconds.
  Value range: "10 ms", "20ms", "30ms", "60ms", "Automatic"
  Default: "Automatic"
- **G.711**: Parameters for the G. 711 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 1"
- **G.729**: Parameters for the G. 729 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Choice 2"
- **G.722**: Parameters for the G. 722 codec.
  Value Range: "Choice 1", "Choice 2", "Choice 3", "Disabled", "Enabled"
  Default: "Disabled"

## Administration via WBM

Speech > Codec preferences




## Administration via Local Phone

- Admin
  - Speech
    - Codec Preferences
      - **Silence suppression**
      - **Packet size**
      - **G.711**
      - **G.729**
      - **G.722**
      - **Allow "HD" icon**

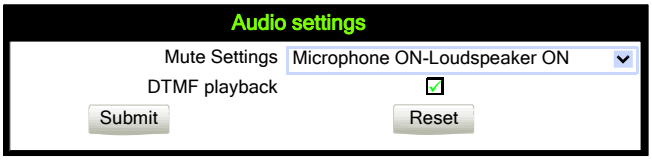
## 3.18.3 Audio Settings

The usage of microphone and speaker for speakerphone mode can be controlled by the administrator.
Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

> The microphone control is not valid for OpenStage 20E, as this model has no built-in microphone.

### Administration via WBM

Speech > Audio Settings




### Administration via Local Phone

- Admin
  - Speech
    - Audio Settings
      - **Disable microphone**
      - **Disable loudspeech**
      - **DTMF playback**

The **DTMF playback** feature aims at the capability to play DTMF digits received using RFC2833 coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker / handset).

# 3.19 Applications

## 3.19.1 XML Applications/Xpressions (OpenStage 60/80)

### 3.19.1.1 Setup/Configuration

The XML interface enables server-based applications with a set of GUI elements. The technologies commonly used in web applications can be used: Java Servlets, JSP, PHP, CGI etc., delivered by servers such as Tomcat, Apache, Microsoft IIS.

A maximum number of 20 XML applications can be configured on OpenStage 60/80 phones.

There are several types of XML applications, which mainly differ in the way they are started and stopped:

- Regular XML applications are started by navigating to the applications menu using the ☰ key, or by pressing a programmable key (see Section 3.8.29, “Start Application”). They can be stopped via the applications menu. Regular XML applications are configured via **Applications** > **XML applications** > **Add application**.
- Xpressions is a special Unified Communications application which also uses the XML interface. Thus, the configuration is just the same as with other XML applications, except a few parameters, which are pre-configured. For details, please refer to the relevant Xpressions documentation. When configured on the phone, a press on the messages mode key ✉ will invoke this application. Xpressions is configured via **Applications** > **XML applications** > **Xpressions**.
- A messages application is configured like a regular application. It is started and stopped via the messages mode key ✉, thus enabling the deployment of an alternative voicemail server. From firmware version V2R1 onwards, the XML application can control the white LED which indicates new messages. A messages application is configured via **Applications** > **XML applications** > **Add messages application**.
- A phonebook application is configured like a regular application. It is started and stopped via the phonebook mode key 🕮, thus enabling the deployment of a remote phonebook in place of the personal (local) or corporate (LDAP) phonebook. A phonebook application is configured via **Applications** > **XML applications** > **Add phonebook application.**
- A call log application is configured like a regular application. It is is started and stopped via the call log mode key ✆, thus enabling the deployment of a remote application that handles call history. From firmware version V2R1 onwards, the XML application can control the white LED which indicates missed calls. A call log application is configured via **Applications** > **XML applications** > **Add call log application**.
- A help application (OS60/80 only) is configured like a regular application. It is is started and stopped via the help mode key ?, thus enabling the deployment of a remote help. A help application is configured via **Applications** > **XML applications** > **Add help application**.

For detailed information about the OpenStage XML application interface, please see the OpenStage 60/80 - XML Applications Developer's Guide. You can find the current version under http://wiki.unify.com/index.php/OpenStage_XML_Applications .

To set up a new XML application, enter the access data for the application on the server, which is described in the following.

The **Display name** can be defined freely. This name will appear in the applications tab once the application is configured, and it will appear in a newly created tab when the application is running. With Xpressions, this value is predefined as "Xpressions".

The **Application name** is used by the phone software to identify the XML application running on the phone. With Xpressions, this value is predefined as "Xpressions".

The **HTTP Server address** is the IP address or domain name of the server which hosts the remote program. **HTTP Server port** specifies the corresponding port.

The **Protocol** for exchanging XML data with the server-side program can be set to "HTTP" or "HTTPS".

**Program name on server** specifies the relative path to the servlet or to the first XML page of the application on the server. The relative path refers to the root directory for documents on the web server. For instance, if an XML document is saved in:
`C:\Program Files\Apache Group\Apache\htdocs\ipp\ippTest.xml`
the entry is:
`ipp/ippTest.xml`.
The program name cannot be longer than 100 characters.

**Auto start** determines whether the application is started automatically on phone startup or on mobile user logon. Please note that, for being started on logon, the application must be part of the mobile user's profile. When activated, the application will be ready without delay as soon as the user presses the corresponding start key or navigates to the application in the application menu.

**Use proxy** enables an HTTP/HTTPS proxy for communication with the server, if desired. If disabled, a direct connection is used.

**XML trace enabled** determines whether debugging information is sent to a special debugging program on the remote server. The relative path for the debugging program is given by the **Debug program name** parameter. When enabled, trace information about the XML elements and key internal objects is sent to the remote debug program.

**Debug program name** specifies the relative path to a special program on the same server as the program specified by **Program name**. This program must be able to receive the debug information sent by the phone as HTTP/HTTPS POST requests with `Content-Type` set to `application/x-www-form-urlencoded`.

XML applications can have internal tabs, if desired. The number of these tabs is specified in **Number of tabs**.

For an XML application with a number of tabs > 0, one of the entries between **Tab 1 Application Name** and **Tab 3 Application Name** must be set to the same value as the **Application name** that it is associated with. When the XML application is started, the tab which has the same name as the XML application is the tab that initially gets focus.

**All tabs start** determines whether all tabs of the application are started automatically when the application is started.

**Tab 1...3 Display Name** provides the label text for the corresponding tab.

**Tab 1...3 Application Name** is required if the application has internal tabs. This is a unique name for the specified tab. The remote program will use this name to provide the tab with specific content.

**Auto restart** / **Restart after change** : If checked, a running XML application is automatically restarted after it has been modified. This might be especially useful for special XML applications, like messages applications, or phonebook applications, as these cannot be stopped or restarted by the user. Please note that a restart will take place even if no changes have been made for the application selected in the **Modify/Delete application** mask, and **Submit** has been pressed. After the XML application has restarted, this option is automatically unchecked. If the option is checked whilst the XML application is not running, there will be no restart, and the option is automatically unchecked.

**Data required**

- **Display name**: Program name to be displayed on the phone.
  Value specifications:
  - It must be unique on the phone.
  - It cannot contain the '^' character.
  - It cannot not be empty.
  - Its length cannot not exceed 20 characters.

- **Application name**: Used internally to identify the XML application running on the phone.
  Value specifications:
  - It must be unique on the phone.
  - It cannot contain non-alphanumeric characters, spaces for instance.
  - The first character must be a letter.
  - It must not be empty.
  - Its length must not exceed 20 characters.
- **Protocol**: Communication protocol for the data exchange with the server.
  Value range: "HTTP", "HTTPS"
  Default: "HTTPS"
- **HTTP Server address**: IP address or domain/host name of the server that provides the application or the XML document.
  Examples: `192.168.1.133`, `backoffice.intranet`
- **Server port number**: Number of the port that the server uses to provide the application or XML document.
  Examples: `80` (Apache default port), `8080` (Tomcat default port).
- **Program name**: Relative path to the servlet or to the first XML page of the application on the server. For instance, if an XML document is saved in:
  `C:\Program Files\Apache Group\Apache\htdocs\ipp\ippTest.xml`
  the entry is:
  `ipp/ippTest.xml`
  The program name cannot be longer than 100 characters.
- **Use proxy**: Enables or disables an HTTP/HTTPS proxy for communication with the server.
  Value range: "Yes", "No"
  Default: "No"
- **XML trace enabled**: Enables or disables the debugging of the XML application.
  Value range: "Yes", "No"
  Default: "No"
- **Debug program name**: The relative path to a special servlet that receives the debug information.

### Administration via WBM

A fixed function key can be defined as a start key for an XML application, in addition to the previously available start methods. Since the parameters are the same for those types of application, only the screenshot for a regular XML application is shown underneath.

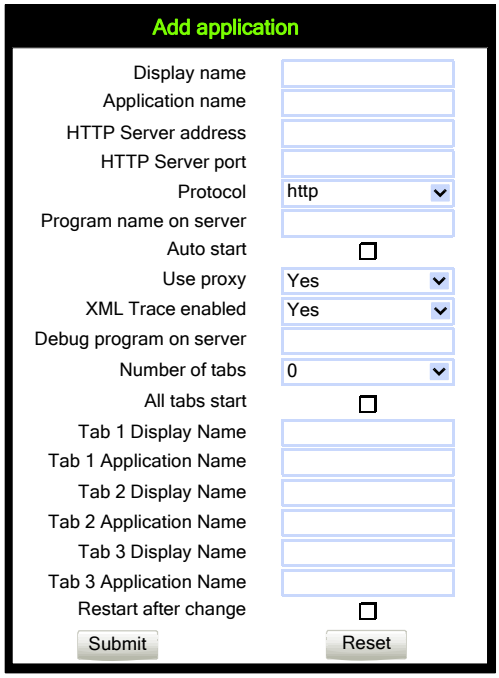
Applications > XML Applications > Add application

Applications > XML Applications > Add messages application

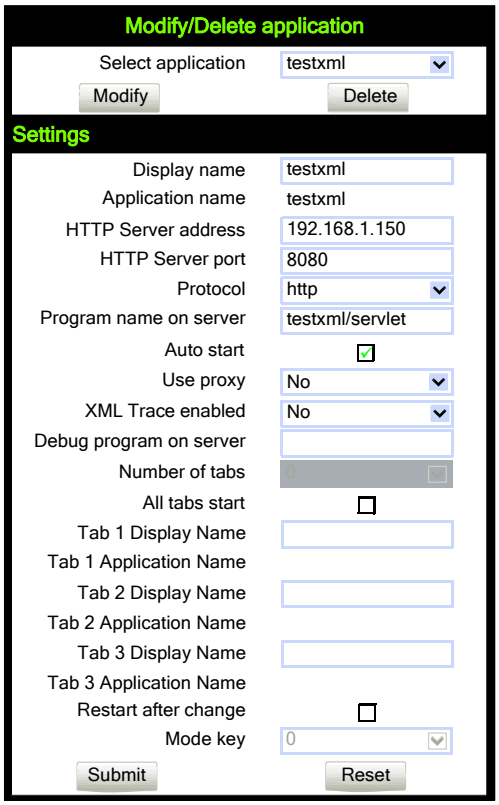
Applications > XML Applications > Add phonebook application

## Applications > XML Applications > Add call log application

## Applications > XML Applications > Add help application




## Applications > XML Applications > Modify/Delete application



### Administration via Local Phone

- Admin
  - Applications
    - XML
      - Add application
        - **Display name**
        - **Application name**
        - **Server address**
        - **Server port**
        - **Protocol**
        - **Program name**
        - **Auto start**
        - **Use proxy**
        - **XML trace enabled**
        - **All tabs start**
        - **Debug program name**
        - **Number of tabs**
        - **Tab 1 display name**
        - **Tab 1 application name**
        - **Tab 2 display name**
        - **Tab 2 application name**
        - **Tab 3 display name**
        - **Tab 3 application name**
        - **Restart after change**

### 3.19.1.2 HTTP Proxy

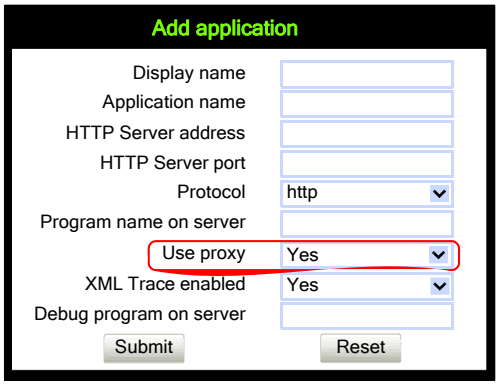
For the HTTP data transfer between the phone and the server hosting the remote program, an HTTP proxy can be used.

First, the proxy itself must be configured. Enter the IP address of the proxy it in the Network > IP configuration > HTTP proxy parameter, and the corresponding port in the Network > Port configuration > HTTP proxy parameter.

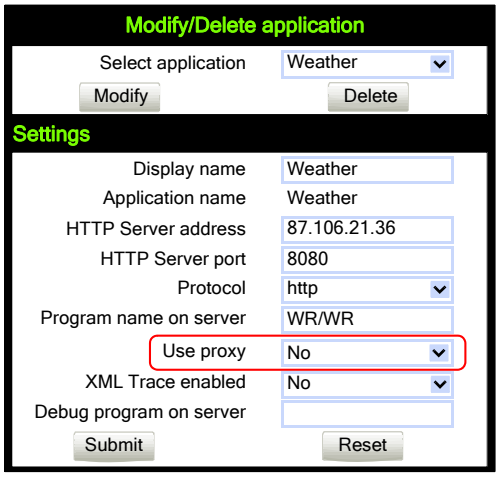
**Use proxy** enables or disables the use of the proxy. If disabled, the phone connects directly to the server. By default, the use of a proxy is disabled.

#### Administration via WBM

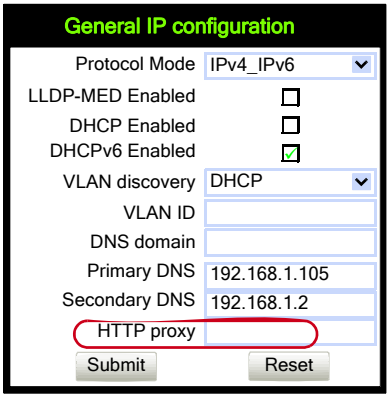
Applications > XML Applications > Add application



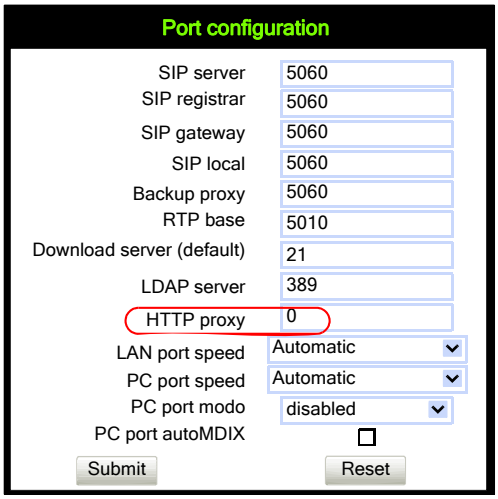

Applications > XML Applications > Modify/Delete application



Network > General IP configuration




Network > Port configuration




## Administration via Local Phone

└── Admin
  └── Network
    └── General IP configuration
      └── **HTTP proxy**

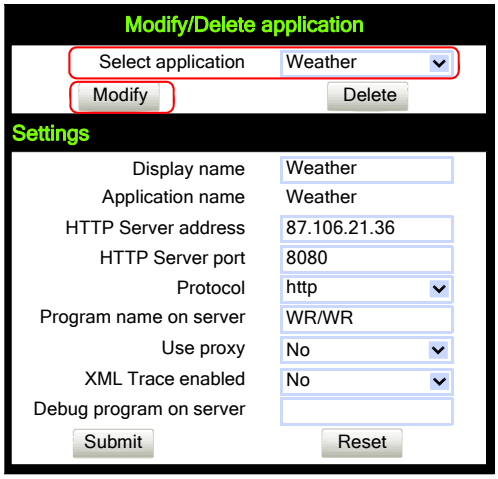
└── Admin
  └── Network
    └── Port configuration
      └── **HTTP proxy**

### 3.19.1.3 Modify an Existing Application

An existing application can be modified by changing its parameters. Please ensure to select the desired application before changing the parameters.

#### Administration via WBM

Applications > XML applications > Modify/Delete application




#### Administration via Local Phone

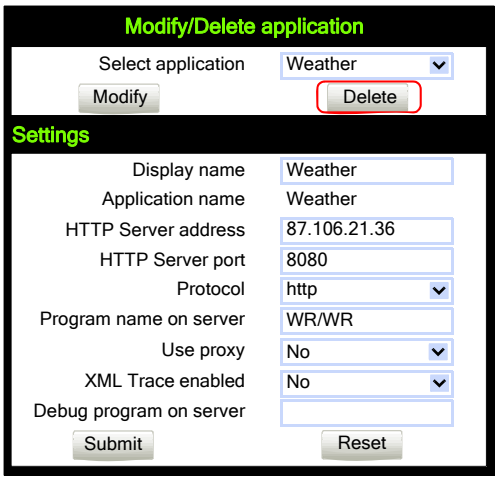
```
└── Admin
    └── Applications
        └── XML
            └── <Application to be modified>
                ├── Display name
                ├── Application name
                ├── Server address
                ├── Server port
                ├── Protocol
                ├── Program name
                ├── XML trace enabled
                └── Debug program name
```

### 3.19.1.4 Remove an Existing Application

An existing application can be removed. Please ensure to select the desired application before changing the parameters.

#### Administration via WBM

Applications > XML applications > Modify/Delete application




#### Administration via Local Phone

Select the application to be deleted, and, in the context menu, select **Remove & exit**.

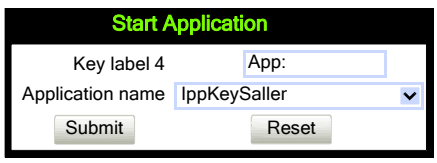
```
└--- Admin
     └--- Applications
          └--- XML
               └--- <Application to be deleted>
```

### 3.19.1.5 Application Start by Programmable Key

To offer more convenience to the user, a previously configured application can be started by a free programmable key. For this purpose, the appropriate **Application name** and a **Key label** must be entered.

#### Administration via WBM

System > Features > Program keys

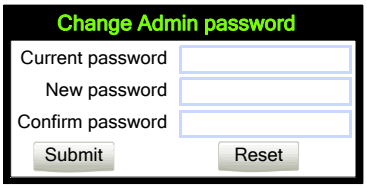


## 3.20 Password

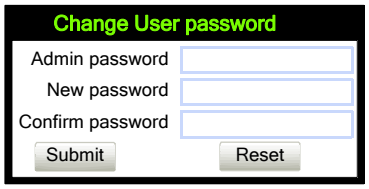
The passwords for user and administrator can be set here. They have to be confirmed after entering. The factory setting is "123456"; it should be changed after the first login (Password handling V2R2 onwards see Section 3.4.5.5, “Change Admin and User password”). Usable characters are 0-9 A-Z a-z .*#,?!’+-()@/:_

### Administration via WBM

Security and Policies > Password > Change Admin password




Security and Policies > Password > Change User password




### Administration via Local Phone

- Admin
  - Security & policies
    - Password
      - **Change admin password**
      - **Change user password**
      - **Confirmation**

## 3.21 Troubleshooting: Lost Password

If the administration and/or user password is lost, and there is no DLS available, new passwords must be provided. For this purpose, a factory reset is necessary. Take the following steps to initiate a factory reset:

1. Press the number keys 2-8-9 simultaneously. The factory reset menu opens.

> The **Factory reset claw** option needs to be enabled for this to work - see Section 3.4.2, “Access Control”.

2. In the input field, enter the special password for factory reset: "124816".
3. Confirm by pressing OK.

## 3.22 Restart Phone

If necessary, the phone can be restarted from the administration menu.

### Administration via WBM

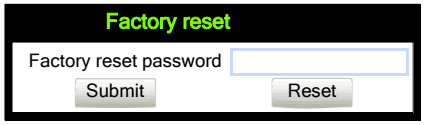
Maintenance > Restart Phone

## 3.23 Factory Reset

This function resets all parameters to their factory settings. A special reset password is required for this operation: "124816".

### Administration via WBM

Maintenance > Factory reset




### Administration via Local Phone

└── Admin
  └── Maintenance
    └── **Factory reset**

## 3.24 SSH – Secure Shell Access

The phone's operating system can be accessed via SSH for special troubleshooting tasks. As of V3, administration via DLS is also supported. Hereby, the administrator is enabled to use the built-in Linux commands. As soon as SSH access has been enabled using the WBM, the system can be accessed by the user "admin" for a specified timespan. When this timespan has expired, no connection is possible any more. The user "admin" has the following permissions:

- Log folder and files: read only
- User data folder and files: read/write access
- Opera deploy folders and files: read only
- Version folder: read/write access; version files: read only

It is not possible to logon as root via SSH.

When **Enable access** is enabled, and the parameters described underneath are specified, SSH access is activated. By default, SSH access is disabled.

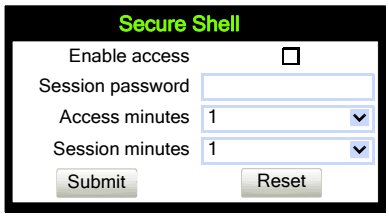
With the **Session password** parameter, a password for the "admin" user is created. This password is required. It will be valid for the timespan specified in the parameters described underneath.

**Access minutes** defines the timespan in minutes within which the SSH connection must be established. After it has expired, a logon via SSH is not possible. The possible values (as of V3) are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

**Session minutes** defines the maximum length in minutes for an SSH connection. After it has expired, the "admin" user is logged out. The possible values are 5, 10, 20, 30, 60.

### Administration via WBM

Maintenance > Secure Shell



## 3.25 Display License Information

The license information for the OpenStage phone software currently loaded can be viewed via the local menu.

The license information can also be viewed by users who logged on using the User login if logging on as Admin is not permitted.

**Administration via Local Phone**

Admin
**Licence information**

## 3.26 Diagnostics

Some of the diagnostic tools and functions may reveal personal data of the user, such as caller lists. Thus, with regards to data privacy, it is recommended to inform the user when diagnostic functions are to be executed.

### 3.26.1 Display General Phone Information

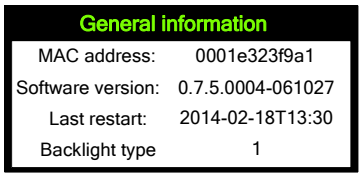
General information about the status of the phone can be displayed if desired.

#### Displayed Data

- **MAC address**: Shows the phone's MAC address.
- **Software version**: Displays the version of the phone's firmware.
- **Last restart**: Shows date and time of the last reboot.
- **Backlight type** : Indicates whether the phone has a backlight, and, if applicable, the type of backlight.
  Value range: 0 (no backlight); 1 (cathode tube backlight); 2 (LED backlight)

#### Display on the WBM

General information




#### Display on the Local Phone

└--- Admin
  └--- General Information
    |--- **MAC address**
    |--- **Software version**
    |--- **Last restart**
    |--- **Dial plan ID**
    └--- **Dial plan status**

## 3.26.2 View Diagnostic Information

In addition to the general phone information (see Section 3.26.1, “Display General Phone Information”), extended data can be viewed.

The Diagnostic Information can also be viewed by the administrator on the local phone by selecting **Diagnostic information > View**.

**Display on the WBM**

Diagnostics > Diagnostic information > View

View

2011-10-16 20:22:33

| | |
|---|---|
| 00 Terminal number: | 3339 |
| 01 SIP server: | 192.168.1.230 |
| 02 SIP port: | 5060 |
| 03 SIP registrar: | 192.168.1.230 |
| 04 SIP registrar port | 5060 |
| 05 SIP gateway: | 192.168.1.230 |
| 06 SIP gateway port | 5060 |
| 07 SIP transport: | UDP |
| 08 SIP local: | 5060 |
| 09 Server features: | No |
| 10 DNS results: | 5060 |
| 11 Multiline: | No |
| 12 Registered lines: | 5060 |
| 13 Backup active: | Yes |
| 14 Backup proxy: | 192.168.1.148 |
| 15 Use secure calls: | No |
| 16 SDES status: | 0 |
| 17 Secure SIP server: | 0 |
| 18 Software version: | V3R0.50.0 110924 |
| 19 Display message: | None |
| 20 Last restart: | 2011-10-10T23:59:01 |
| 21 Memory free: | 65733K free |
| 22 Protocol mode: | IPv4 |
| 23 IP4 address: | 192.168.1.235 |
| 24 IP4 subnet mask: | 255.255.255.0 |
| 25 IP4 default route: | 192.168.1.2 |
| 26 Primary DNS: | 192.168.1.105 |
| 27 Secondary DNS: | 192.168.1.2 |
| 28 IP4 route 1 IP: | None |
| 29 IP4 route 1 gateway: | None |
| 30 IP4 route 1 mask: | None |
| 31 IP4 route 2 IP: | None |
| 32 IP4 route 2 gateway: | None |
| 33 IP4 route 2 mask: | None |
| 34 IP6 address: | None |
| 35 IP6 prefix length: | None |
| 36 IP6 global gateway: | None |
| 37 IP6 link local addr: | None |
| 38 IP6 route 1 dest: | None |
| 39 IP6 route 1 pref len: | None |
| 40 IP6 route 1 gateway: | None |
| 41 IP6 route 2 dest: | None |
| 42 IP6 route 2 pref len: | None |
| 43 IP6 route 2 gateway: | None |
| 44 MAC address: | 0001e325eaca |
| 45 Discovery mode: | Manual |
| 46 DHCP re-use: | No |
| 47 DHCPv6: | Yes |
| 48 DHCPv6 re-use: | No |
| 49 LAN port type: | 0 |
| 50 PC port status: | None |
| 51 PC port type: | 0 |
| 52 PC port autoMDIX: | No |
| 53 VLAN ID: | None |
| 54 QoS Layer 2: | None |
| 55 QoS Layer 2 voice: | 5 |
| 56 QoS Layer 2 signalling: | None |
| 57 QoS Layer 2 default: | 0 |
| 58 QoS Layer 3: | Yes |
| 59 QoS Layer 3 voice: | EF / 46 |
| 60 QoS Layer 3 signalling: | AF31 / 26 |
| 61 LLDP-MED operation: | None |

62 XML application:
None
63 XML app config:

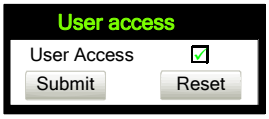
## 3.26.3 User Access to Diagnostic Information

If this option is enabled, extended phone data is also displayed to the user. To view the data, the user must click on the "Diagnostic information" link in the user menu.

The Diagnostic Information can also be viewed by the user on the local phone by selecting **User > Diagnostic information**.

### Administration via WBM

Diagnostics > Diagnostic information > User access




## 3.26.4 Diagnostic Call

The feature "Rapid Status Diagnostic Call" will provide the possibility to place a diagnostic call, for example by the user, which starts call related tracing on the phone and on involved OpenScape Voice and collect these traces at OpenScape Voice Trace Manager (OSVTM). With all these traces available, a call can be followed throughout the voice system and a possible problem can be detected faster. As all traces from all involved components are available at the first level support, the analysis of a possible problem can be started immediately.

A so-called diagnostic scenario will enable traces on all involved SIP components of the OSC Voice solution and store all traces at a central server. A tool will help service to follow a call through the traces and determine the point of problem.

The approach is to use a SIP Header ([1]) to indicate, whether a call is a diagnostic call or not. Presence of this header will mean that related call is a diagnostic call. Absence of this field means a non-diagnostic call. This header will either switch on traces in the solution component or be ignored, if it isn't supported. If the call is recognized as a diagnostic call, the traces will be sent to DLS as a first step and then DLS will forward them to OSVTM. Collected traces will either be sent after a successful end of diagnostic scenario or trace file is full.

For enabling tracing on all involved solution components, a call must be recognized to be a "diagnostic" call. Therefore, a special SIP header will be added to the signalling messages. All components which are able to support such a call will then switch on traces and send the traces to DLS server (which will forward them to a pre-defined OSVTM server).

A dial-prefix has been chosen, as the dialled number should be identical to a number, where the user identified a possible problem. This prefix will be filtered before placing a call, so that the SIP messages will be similar to the ones for the problematic destination.

The SIP header "X-Siemens-Trace-ID" has been chosen, as this is a special SIP field created for this feature. Existence of the diagnostic call, start and finish of a diagnostic call can be determined via this field [1].

Trace id will be unique throughout the system and the following format will be used to generate trace id:

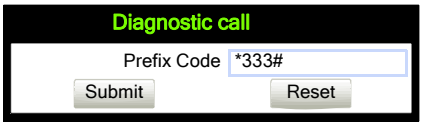
`TraceId: <UNIX_Timestamp>_<Last 6 bytes of MAC Address>`

If related calls (diagnostic or not) are established following the start of the diagnostic call, then it turns to be a diagnostic scenario. Related calls become diagnostic (if they are not already) and traces are collected until the last diagnostic call ends plus a predefined timer. This timer guarantees capturing related information regarding to a problematic scenario.

The diagnostic call can only be determined during the call so initial traces might get lost. For this reason, user may need to do additional call. This is completely user related and user should be informed about the process. There will not be any restriction to prevent user to dial the prefix. If the prefix is configured by admin, user can always dial the prefix and start a diagnostic call. The prefix has to consist of the leading asterisk followed by three digits and the hash. Example: *333#.

### Administration via WBM

Maintenance > Diagnostic call




### Administration via Local Phone

└--- Admin
  └--- Maintenance
    └--- **Diagnostic Call**

Admin will not be able to change trace settings or can not clear the existing phone traces during an active diagnostic tracing. If admin tries to change trace configuration or delete existing traces this will not be allowed and admin will get the following error: **Change not allowed: Diagnostic tracing is active!**

### 3.26.5 LAN Monitoring

The LAN port mirror facility allows for monitoring all network traffic at the phone's LAN port.

Additionally, there is a possibility to monitor LAN traffic and port settings in the Local user menu:

- User
  - Network information
    - **Phone address**
    - **Web address**
    - **IPv4 address**
    - **IPv6 Global Address**
    - **IPv6 Linklocal Address**
    - **LAN RX**
    - **LAN TX**
    - **PC RX**
    - **PC TX**
    - **LAN autonegotiated**
    - **LAN information**
    - **PC autonegotiated**
    - **PC information**

## 3.26.6 LLDP-MED

When the phone is connected to a switch with LLDP-MED capabilities, it can receive a VLAN ID and QoS parameters and advertise its own network-related properties. The data is exchanged in TLV (Type-Length-Value) format.

Both sent and received LLDP-MED data can be monitored at the administrator interface.

For details on LLDP-MED, please refer to the ANSI/TIA-1057 standard.

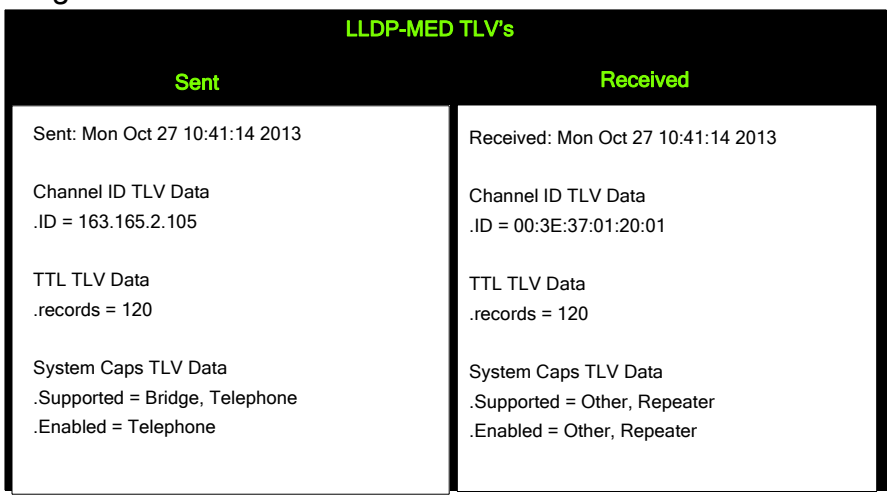
For a network configuration example that shows LLDP-MED in operation, please refer to Section 5.4, “An LLDP-Med Example”.

### Displayed Data

- **Extended Power**: Power Consumption; relevant for PoE.
- **Network policy (voice)**: VLAN ID and QoS (Quality of Service) parameters for voice transport.
- **Network policy (signalling)**: VLAN ID and QoS (Quality of Service) parameters for signalling.
- **LLDP-MED capabilities**: The LLDP-MED TLVs supported by the phone and the switch as well as the specific device class they belong to.
- **MAC_Phy configuration**: Identifies the possible duplex and bit-rate capability of the sending device, its current duplex and bit-rate capability, and whether theses settings are the result of auto-negotiation during the initialization of the link, or of manual set override actions.
- **System capabilities**: The devices advertise their potential and currently enabled functions, e. g. "Bridge", "Telephone".
- **TTL**: **T**ime **T**o **L**ive. This parameter determines how long the TLVs are valid. When expired, the device will send a new set of TLVs.

### View Data From WBM

Diagnostics > LLDP-MED TLVs




### View Data From Local Menu

If both sent and received values are concordant, **OK** is appended to the parameter. If not, an error message is displayed.

- Admin
  - Network
    - LLDP-MED operation
      - **Extended Power**
      - **Network policy (voice)**
      - **LLDP-MED cap's**
      - **MAC_Phy config**
      - **System cap's**
      - **TTL**

## 3.26.7 IP Tests

For network diagnostics, the OpenStage phone can ping any host or network device to determine whether it is reachable. Additionally, the IP route to a host or network device can be traced using the traceroute tool contained in the phone software.

The **Pre Defined Ping tests** provide pinging for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

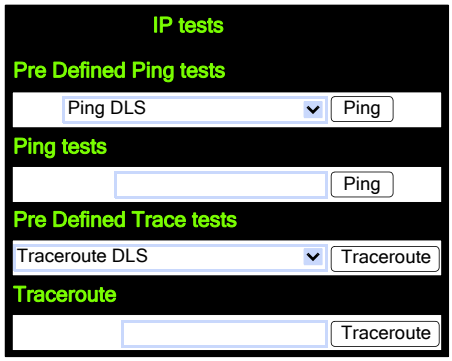
**Ping tests** enables the pinging of a random IP address.

The **Pre Defined Trace tests** provide traceroute tests for a pre-defined selection of servers: DLS, SIP server, and SIP registrar.

**Traceroute** enables traceroute tests for a random IP address.

### Administration via WBM

Diagnostics > Miscellaneous > IP tests



### 3.26.8 Process and Memory Information

The processes currently running on the phone's operating system as well as their CPU and memory usage can be monitored here. 100 processes are monitored on the web page. For further information, please refer to the manual of the "top" command for Unix/Linux systems, or to related documentation.

The amount of free memory is checked on a regular basis in order to prevent problems caused by low memory. This check determines whether a recovery is necessary.

When **Disable reboot** is checked, no reboot will take place when a memory problem has been found. However, recovery requires a reboot.

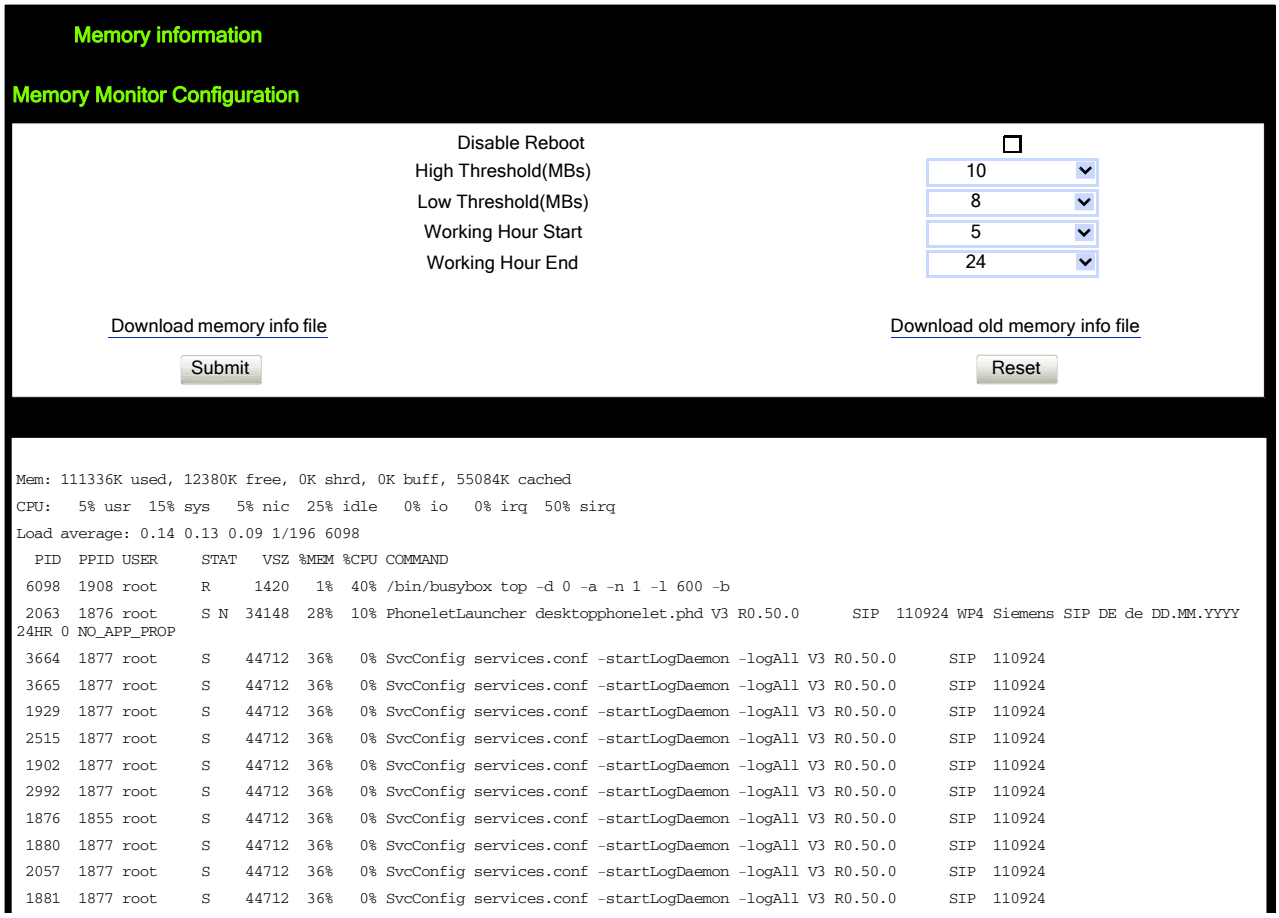
The recovery process will be triggered when the available main memory (RAM) falls below a given threshold value. As memory consumption is assumed to be higher during working hours, two thresholds are configurable. The **High Threshold (MBs)** parameter defines the threshold for off-time. For OpenStage 15/20/40, the default value is 10 MB, and for OpenStage 60/80, it is 30 MB. With **Low Threshold (MBs)**, the threshold for off-time is defined. For OpenStage 15/20/40, the default value is 8 MB, and for OpenStage 60/80, it is 20 MB.

The beginning and end of the working hours are defined in 24 hours format with **Working Hour Start** (Default: 5) and **Working Hour End** (Default: 24).

When memory shortage has occured, information about the incident is written to a log file which can be viewed via the **Download memory info file** link. If there has been a previous case of memory shortage, the corresponding log file can be viewed via **Download memory info file**.

## Administration via WBM

### **Diagnostics** > **Miscellaneous** > Memory information


Memory information
Memory Monitor Configuration
Disable Reboot
High Threshold(MBs)
10
Low Threshold(MBs)
8
Working Hour Start
5
Working Hour End
24
Download memory info file
Download old memory info file
Submit
Reset
Mem: 111336K used, 12380K free, 0K shrd, 0K buff, 55084K cached
CPU: 5% usr 15% sys 5% nic 25% idle 0% io 0% irq 50% sirq
Load average: 0.14 0.13 0.09 1/196 6098
PID PPID USER STAT VSZ %MEM %CPU COMMAND
6098 1908 root R 1420 1% 40% /bin/busybox top -d 0 -a -n 1 -l 600 -b
2063 1876 root S N 34148 28% 10% PhoneletLauncher desktopphonelet.phd V3 R0.50.0 SIP 110924 WP4 Siemens SIP DE de DD.MM.YYYY 24HR 0 NO_APP_PROP
3664 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
3665 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1929 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2515 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1902 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2992 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1876 1855 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1880 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2057 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1881 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924

### 3.26.9 Fault Trace Configuration

Error tracing and logging can be configured separately for all components, i. e. the services and applications running on the OpenStage phone. The resulting files can be viewed in the WBM web pages over the **Download** links.

The **File size (bytes)** parameter sets the maximum file size. When it is reached, the data is saved as old file, and a new file is generated. From then on, the trace data is written to the new file. When the maximum file size is reached again, the data is saved as old file once more, thereby overwriting the previous old file. The default value is 65536.

The absolute maximum file size is 6290000 bytes. However, on OpenStage 15/20/40 phones, a maximum size no greater than 1000 000 bytes is recommended due to the amount of available memory.

The **Trace timeout (minutes)** determines when to stop tracing. When the timeout is reached, the trace settings for all components are set to OFF, but ERROR and STATUS messages are still written to the trace file ad infinitum. When the trace file has reached its maximum size, the data is saved, and a new file is created (for more information, see **File size (bytes)** above). If the value is 0, the trace data will be written without time limit.

If **Automatic clear before start** is checked, the existing trace file will be deleted on pressing the **Submit** button, and a new, empty trace file will be generated. By default, it is unchecked.

You can read the log files by clicking on the appropriate hyperlinks (the hyperlinks work only if the file in question has been created). The following logs can be viewed:

- **Download trace file**
  The trace data according to the settings specified for the services.
- **Download old trace file**
  The trace file is stored in permanent memory. When the file has reached its size limit, it will be saved as old trace file, and the current exception file is emptied for future messages. The old trace file can be viewed here.
- **Download saved trace file**
  Normally, the trace file is saved only in the phone RAM. When the phone restarts in a controlled manner, the trace file will be saved in permanent memory.
- **Download syslog file**
  Messages from the phone's operating system, including error and exception messages.
- **Download old syslog file**
  Old messages from the phone's operating system.
- **Download saved syslog file**
  Saved messages from the phone's operating system.
- **Download exception file**
  If an exceptions occurs in a process running on the phone, a message is written to this file. These messages are incorporated in the syslog file (see **Download syslog file** also).

- **Download old exception file**
  The exception file is stored permanent memory. When the file has reached its size limit, it will be saved as old exception file, and the current exception file is emptied for future messages. The old exception file can be viewed here.
- **Download upgrade trace file**
  The trace log created during a software upgrade.
- **Download upgrade error file**
  The error messages created during a software upgrade. These messages are incorporated in the syslog file (see **Download syslog file** also).
- **Download dial plan file**
  If a dial plan has been uploaded to the phone, it is displayed here, along with its status (enabled/disabled) and error status. For details, please refer to Section 3.13.4, “Dial Plan” and Section 5.5, “Dial Plan”.
- **Download Database file**
  Configuration parameters of the phone in SQLite format.
- **Download HPT remote service log file**
  Log data from the HPT service.
- **Download security log file**
  Log data from the Security Log Service.

By pressing **Submit**, the trace settings are submitted to the phone. With **Reset**, the recent changes can be canceled.

The following trace levels can be selected:
- **OFF**: Default value. Only error messages are stored.
- **FATAL**: Only fatal error messages are stored.
- **ERROR**: Error messages are stored.
- **WARNING**: Warning messages are stored.
- **LOG**: Log messages are stored.
- **TRACE**: Trace messages are stored. These contain detailed information about the processes taking place in the phone.
- **DEBUG**: All types of messages are stored.

### Brief Descriptions of the Components/Services

- **Administration**
  Deals with the changing and setting of parameters within the phone database, from both the User and Admin menus.
- **AGP Phonelet**
  Deals with AGP Phonelet.
- **Application framework**

All applications within the phone, e.g. Call view, Call log, or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.

- **Application menu**
  This is where applications to be run on the phone can be started and stopped.
- **Bluetooth service**
  Handles the Bluetooth interactions between external Bluetooth devices and the phone.
  Bluetooth is available only on OpenStage 60/80 phones.
- **Call log**
  The Call log application displays the call history of the phone.
- **Call view**
  Handles the representation of telephony calls on the phone screen.
- **Certificate management**
  Handles the verification and exchange of certificates for security and verification purposes.
- **Clock service**
  Handles the phone's time and date, including daylight saving and NTP functionality.
- **Communications**
  Involved in the passing of call related information and signaling to and from the CSTA service.
- **Component registrar**
  Handles data relating to the type of phone, e.g. OpenStage 20/40 HFA/SIP, OpenStage 60/80 HFA/SIP.
- **CSTA service**
  Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.
- **Data Access service**
  Allows other services to access the data held within the phone database.
- **Desktop**
  Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
- **Digit analysis service**
  Analyses and modifies digit streams which are sent to and received by the phone, e.g. canonical conversion.
- **Directory service**
  Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
- **DLS client management**
  Handles interactions with the DLS (Deployment Service).
- **Health service**

Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.

- **Help**
  Handles the help function.
- **HTTP Service**
  Handles the HTTP Service messages.
- **Instrumentation service**
  Used by the Husim phone tester to exchange data with the phone for remote control, testing and monitoring purposes.
- **Journal service**
  Responsible for saving and retrieving call history information, which is used by the Call log application.
- **Media control service**
  Provides the control of media streams (voice, tones, ringing etc. ) within the phone.
- **Media processing service**
  This is a layer of software between the media control service, the tone generation, and voice engine services. It is also involved in the switching of audio devices such as the handset and loudspeaker.
- **Media recording service**
  Logs the data flow generated with call recording.
- **Mobility service**
  Handles the mobility feature whereby users can log onto different phones and have them configured to their own profile.
- **OBEX service**
  Involved with Bluetooth accesses to the phone.
  Bluetooth is available only on OpenStage 60/80 phones.
- **OpenStage client management**
  Provides a means by which other services within the phone can interact with the database.
- **Password management service**
  Verifies passwords used in the phone.
- **Phonebook**
  Responsible for the phonebook application.
- **Performance Marks**
  Aid for measuring the performance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss yyyy.milliseconds, and information about the event. The timespan between two performance marks is an indicator for the performance of the phone.

The trace level must be set to "TRACE" or "DEBUG".

- **Physical interface service**
  Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, clickwheel and slider.
- **Security Log Service**
  Handles Security Log Service messages.
- **Service framework**
  This is the environment within which other phone services operate. It is involved in the starting and stopping of services.
- **Service registry**
  Keeps a record of all services currently running inside the phone.
- **Sidecar service**
  Handles interactions between the phone and any attached sidecars.
- **SIP call control**
  Contains the call model for the phone and is associated with telephony and call handling.
- **SIP messages**
  Traces the SIP messages exchanged by the phone.

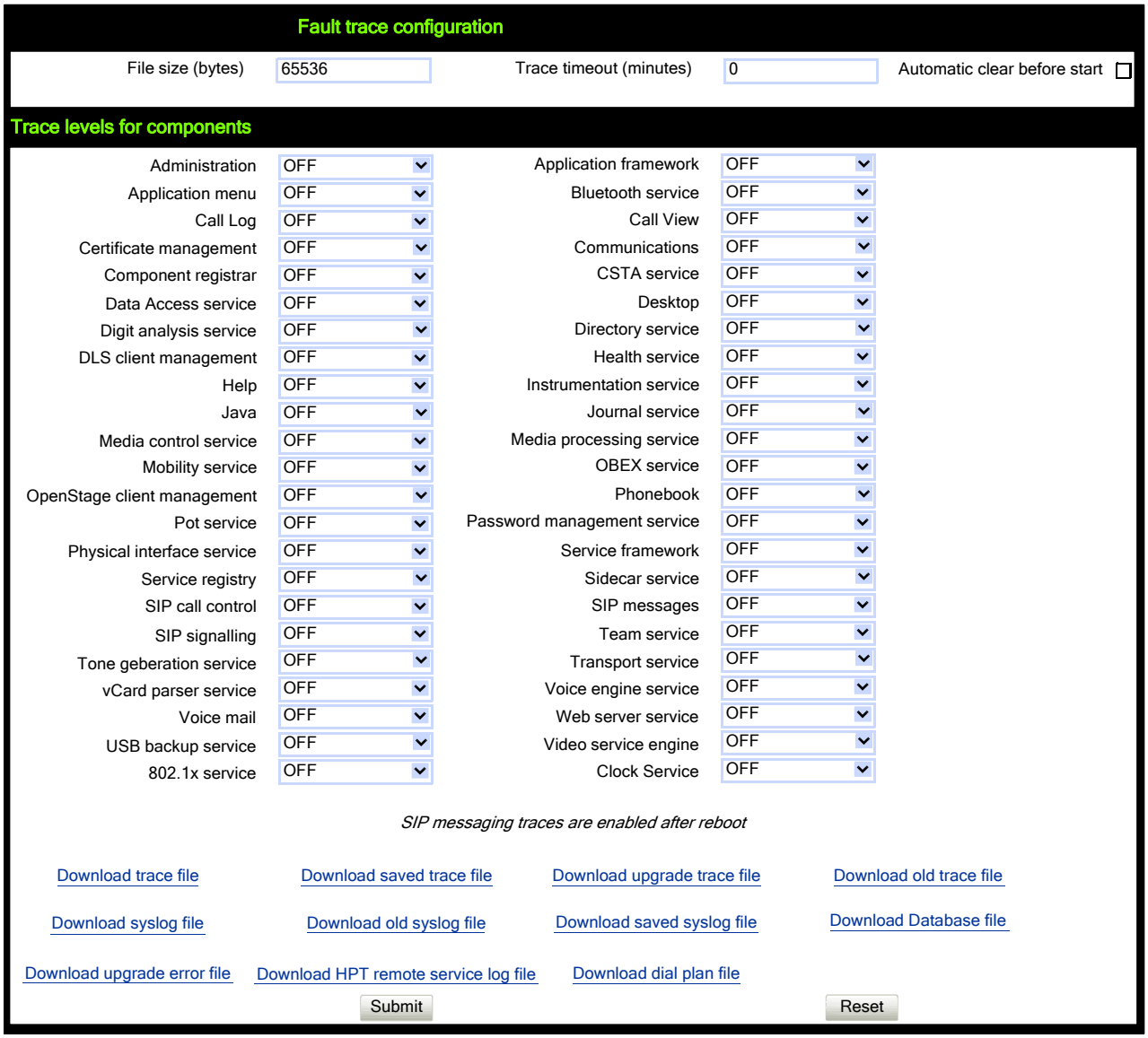
After changing the level for the tracing of SIP messages, the phone must be rebooted. Otherwise the changes would have no effect.

- **SIP signalling**
  Involved in the creation and parsing of SIP messages. This service communicates directly with the SIP stack.
- **Team service**
  Primarily concerned with keyset operation.
- **Tone generation service**
  Handles the generation of the tones and ringers on the phone.
- **Transport service**
  Provides the IP (LAN) interface between the phone and the outside world.
- **USB backup service**
  Used to make backup/restore to/from USB stick by using password. This item is available in the phone GUI.
- **vCard parser service**
  Handles parsing and identification of VCard information while sending or getting VCards via Bluetooth.
- **Voice engine service**
  Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.
- **Voice mail**
  Handles the voice mail functionality.

- **Web server service**
  Provides access to the phone via web browser.
- **802.1x service**
  Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.

## Administration via WBM

### Diagnostics > Fault trace configuration



## 3.26.10 EasyTrace Profiles

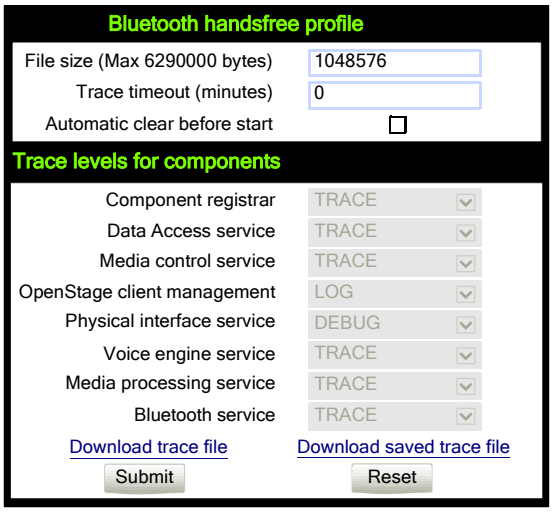
In order to simplify tracing for a specific problem, the tracing levels can be adjusted using pre-defined settings. The EasyTrace profiles provide settings for a specific area, e. g. call connection. On pressing **Submit**, those pre-defined settings are sent to the phone. If desired, the settings can be modified anytime using the general mask for trace configuration under **Diagnostics** > Fault Trace Configuration (see Section 3.26.9, “Fault Trace Configuration”).

If desired, the tracing for all services can be disabled (see Section 3.26.10.26, “No Tracing for All Services”).

The following sections describe the EasyTrace profiles available for the phone.

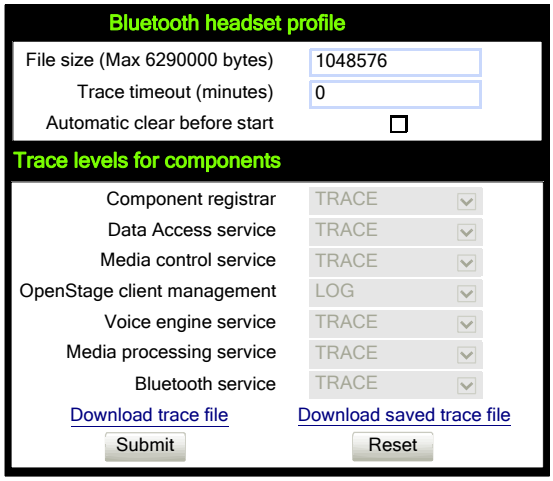
### 3.26.10.1 Bluetooth Handsfree

Diagnostics > EasyTrace Profiles > Bluetooth handsfree profile



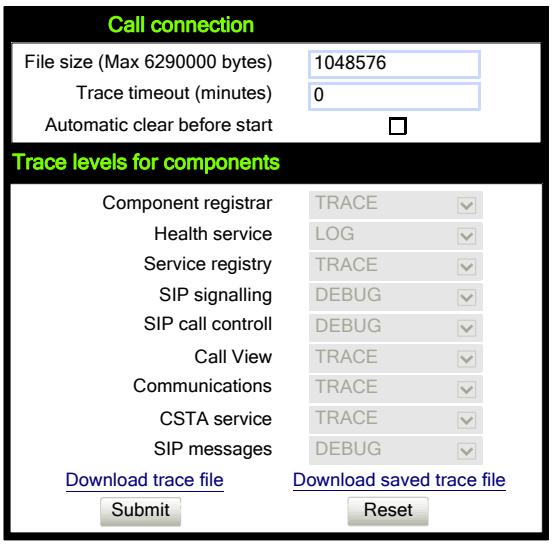
### 3.26.10.2 Bluetooth Headset

Diagnostics > EasyTrace Profiles > Bluetooth headset profile




### 3.26.10.3 Call Connection

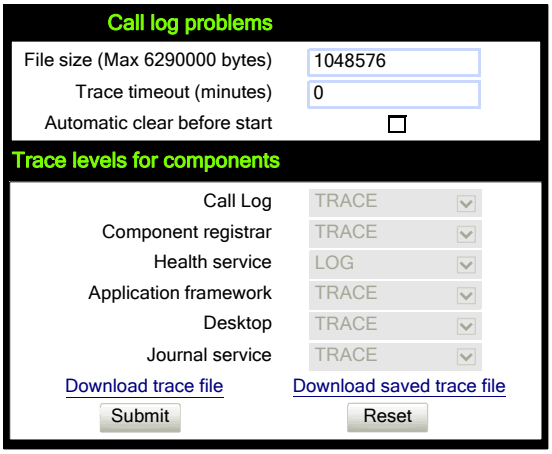
Diagnostics > EasyTrace Profiles > Call connection




This EasyTrace profile contains the tracing of SIP messages. Please note that after changing the level for the tracing of SIP messages, the phone must be rebooted.

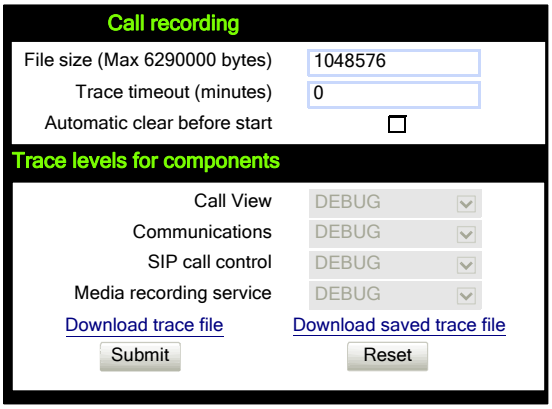
### 3.26.10.4 Call Log

Diagnostics > EasyTrace Profiles > Call log problems



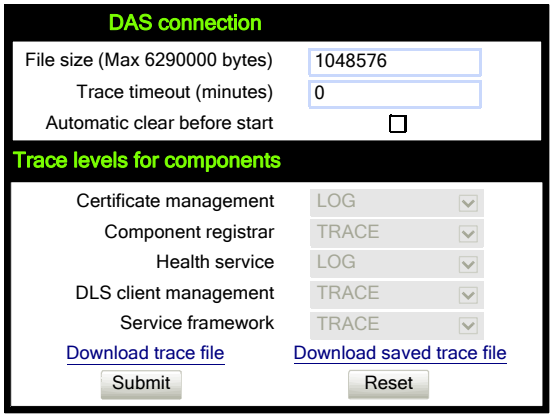

### 3.26.10.5 Call Recording

Diagnostics > EasyTrace Profiles > Call recording



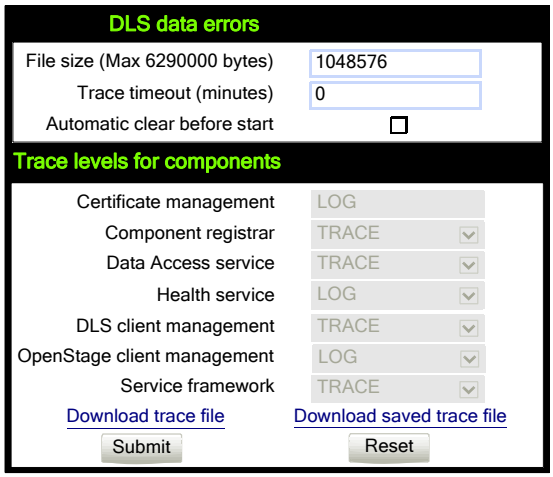
### 3.26.10.6 DAS Connection

Diagnostics > EasyTrace Profiles > DAS connection



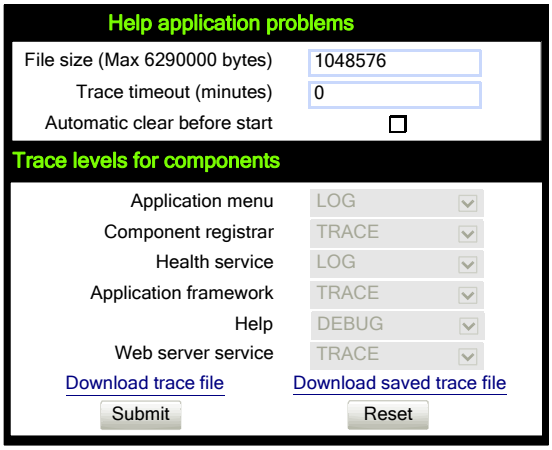

### 3.26.10.7 DLS Data Errors

Diagnostics > EasyTrace Profiles > DLS data errors



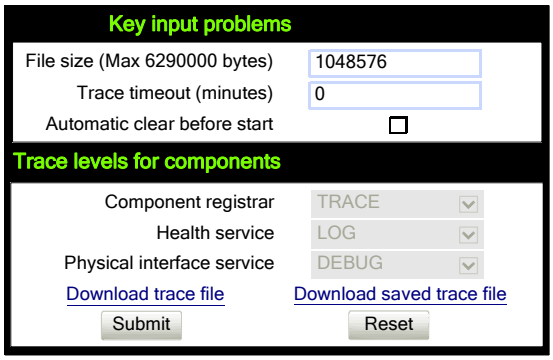
### 3.26.10.8 Help Application

Diagnostics > EasyTrace Profiles > Help application problems



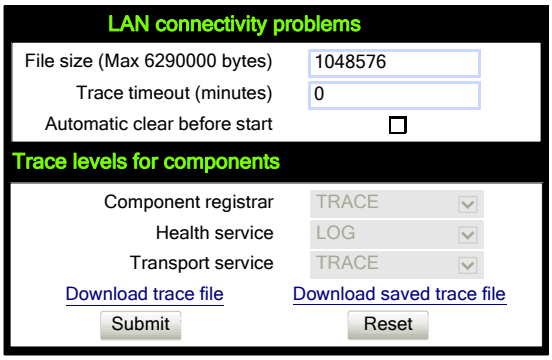

### 3.26.10.9 Key Input

Diagnostics > EasyTrace Profiles > Key input problems



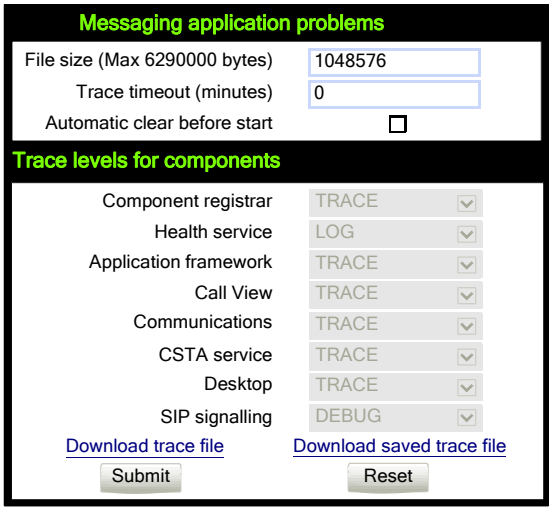
### 3.26.10.10 LAN Connectivity

Diagnostics > EasyTrace Profiles > LAN connectivity problems



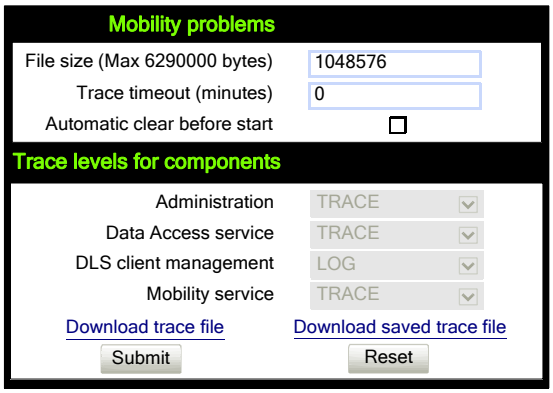

### 3.26.10.11 Messaging

Diagnostics > EasyTrace Profiles > Messaging application problems



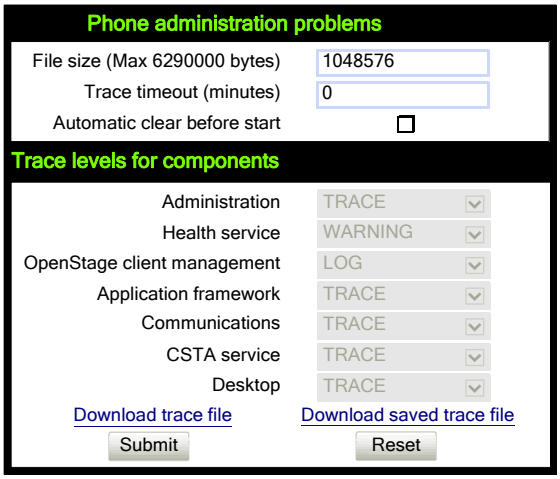
### 3.26.10.12 Mobility

Diagnostics > EasyTrace Profiles > Mobility problems



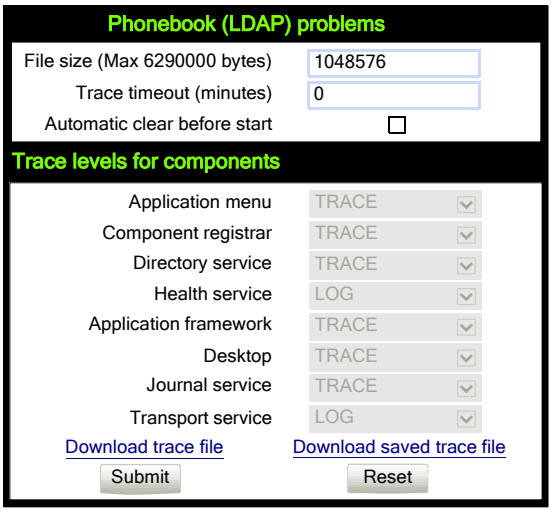

### 3.26.10.13 Phone administration

Diagnostics > EasyTrace Profiles > Phone administration problems



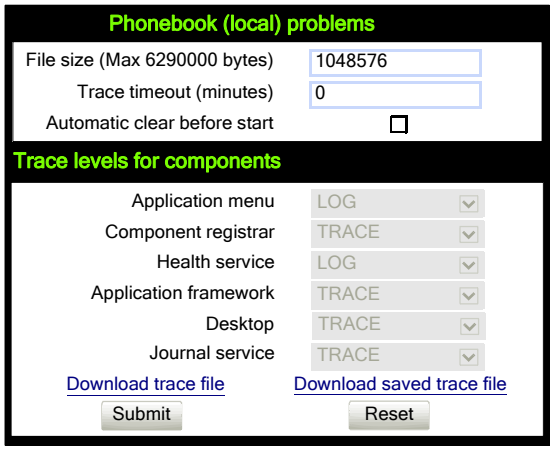
### 3.26.10.14 LDAP Phonebook

Diagnostics > EasyTrace Profiles > Phonebook (LDAP) problems



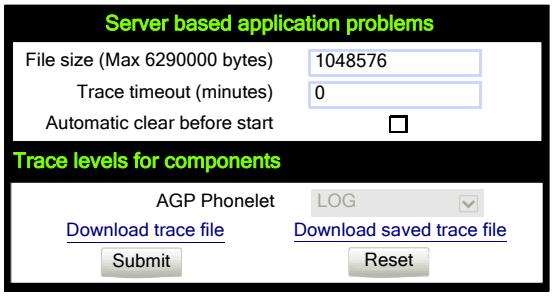

### 3.26.10.15 Local Phonebook

Diagnostics > EasyTrace Profiles > Phonebook (local) problems



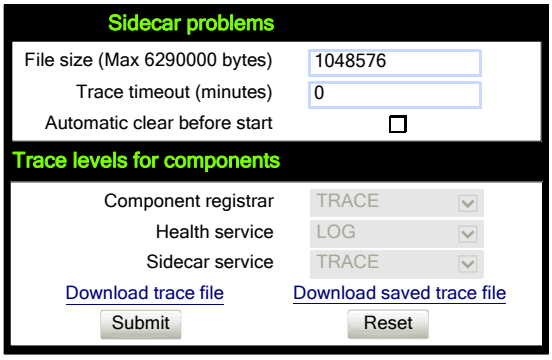
### 3.26.10.16 Server based applications

Diagnostics > EasyTrace Profiles > Server based application problems



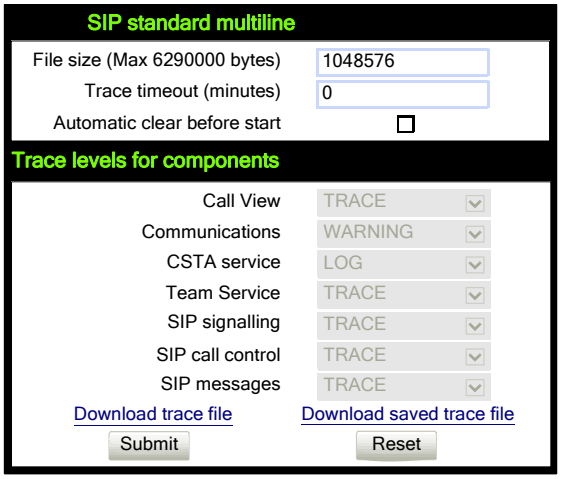

### 3.26.10.17 Sidecar

Diagnostics > EasyTrace Profiles > Sidecar problems



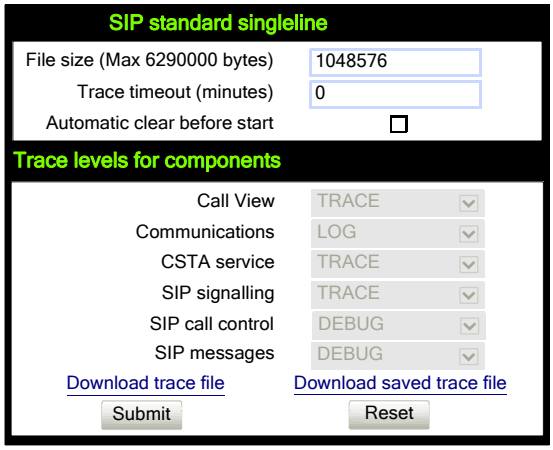
### 3.26.10.18 SIP standard multiline

Diagnostics > EasyTrace Profiles > SIP standard multiline



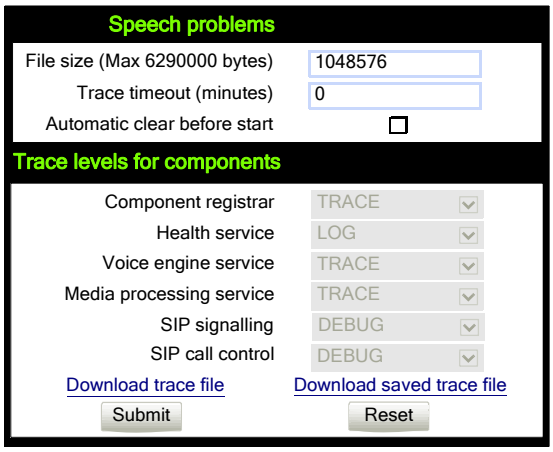

### 3.26.10.19 SIP standard singleline

Diagnostics > EasyTrace Profiles > SIP standard singleline



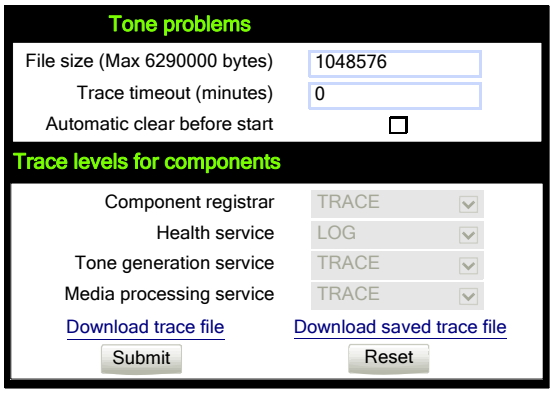
### 3.26.10.20 Speech

Diagnostics > EasyTrace Profiles > Speech problems



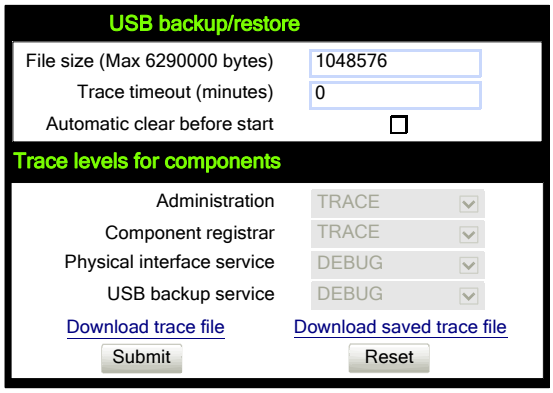

### 3.26.10.21 Tone

Diagnostics > EasyTrace Profiles > Tone problems



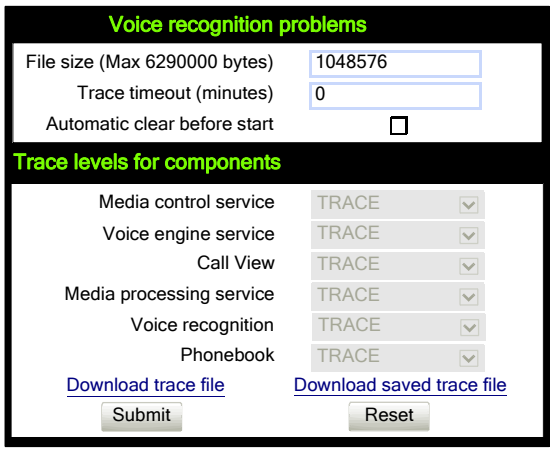
### 3.26.10.22 USB Backup/Restore

Diagnostics > EasyTrace Profiles > USB backup/restore



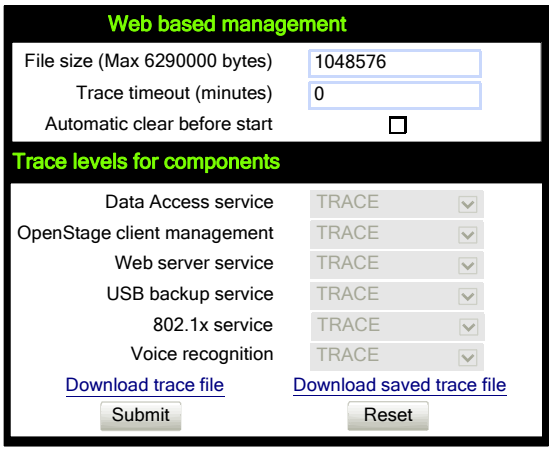

### 3.26.10.23 Voice Dialling

Diagnostics > EasyTrace Profiles > Voice recognition problems



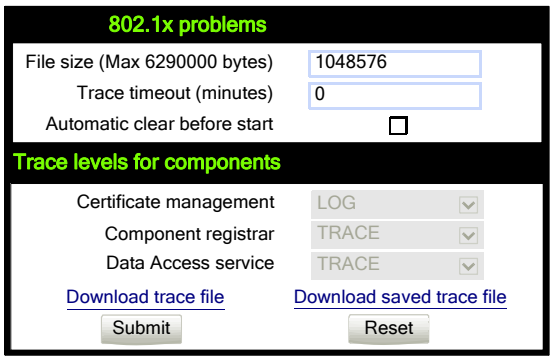
### 3.26.10.24 Web Based Management

Diagnostics > EasyTrace Profiles > Web based management



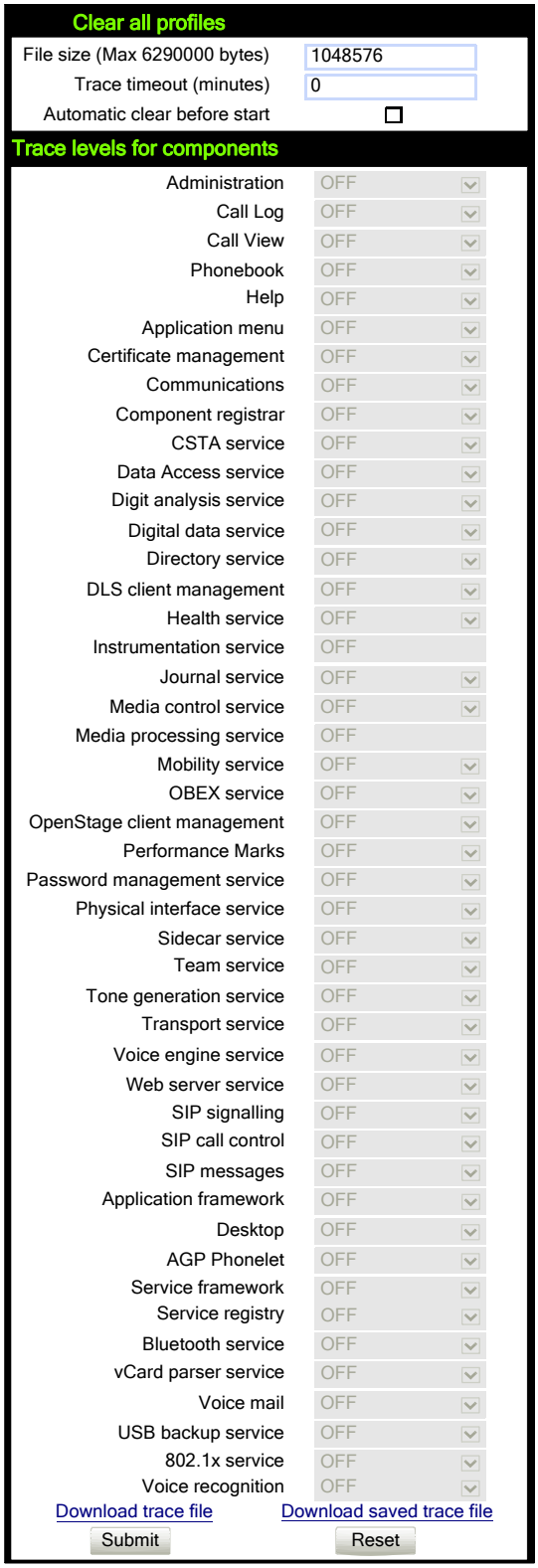

### 3.26.10.25 802.1x problems

Diagnostics > EasyTrace Profiles > 802.1x problems



### 3.26.10.26 No Tracing for All Services

Diagnostics > EasyTrace Profiles > Clear all profiles



## 3.26.11 Bluetooth Advanced Traces

For OpenStage 60/80 phones, low level Bluetooth traces can be controlled and viewed via web interface, in addition to the tracing facilities available in previous firmware versions (see Section 3.26.9, “Fault Trace Configuration”). Internally, the phone uses the hcdump utility for creating the traces. It is also possible to run the trace from the shell via SSH (for information about the SSH access, please refer to Section 3.24, “SSH – Secure Shell Access”).

If **Automatic clear before start** is enabled, the log file will be emptied before the **Start** button is pressed, so that the log file will only containd newly created entries. By default, this parameter is enabled.

The **File size (Max 6290000 bytes)** parameter determines the maximum size of the log file. If this value is exceeded, no more data will be written to the file. The default value is 265536.

If **Extended dump** is enabled, all hexadecimal and ASCII data is displayed for each packet. If disabled, only the packet type is displayed. By default, this parameter is enabled.

If **Verbose decoding** is enabled, the packets are decoded in a more verbose way. By default, this parameter is enabled.

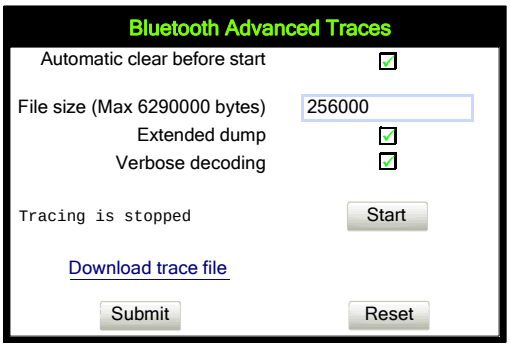
With the **Start**/**Stop** button, tracing is started or halted. The label depends on whether tracing is active or not.

On clicking the **Download trace file** link, the trace file is displayed.

With **Submit**, the changes on the parameters described above are sent to the phone.

With **Reset**, parameter changes that have been made in the form, but not yet sent to the phone, are cancelled.

### Administration via WBM



## 3.26.12 QoS Reports

### 3.26.12.1 Conditions and Thresholds for Report Generation

For details about the functionality, please refer to the release notes.

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see Section 3.3.9, “SNMP”) is configured here.

**Data required**

- **Report mode**: Sets the conditions for generating a QoS report.
  Value range:
  - "OFF": No reports are generated.
  - "EOS Threshold exceeded": Default value. A report is created if a) a telephone conversation longer than the **Minimum session length** has just ended, and b) a threshold value has been exceeded during the conversation.
  - "EOR Threshold exceeded": A report is created if a) the report interval has just passed, and b) a threshold value has been exceeded during the observation interval.
  - "EOS (End of Session)": A report is created if a telephone conversation longer than the **Minimum session length** has just ended.
  - "EOR (End of Report Interval)": A report is created if the report interval has just passed.
- **Report interval (seconds)**: Time interval between the periodical observations.
  Default: 60
- **Observation interval (seconds)**: During this time interval, the traffic is observed.
  Value: 10
- **Minimum session length (100 millisecond units)**: When the Report mode is set to "EOS Threshold exceeded" or "EOS (End of Session)", a report can be created only if the duration of the conversation exceeds this value.
  Default: 20
- **Maximum jitter (milliseconds)**: When the jitter exceeds this value, a report is generated.
  Default: 20
- **Average round trip delay (milliseconds)**: When the average round trip time exceeds this value, a report is generated.
  Default: 100

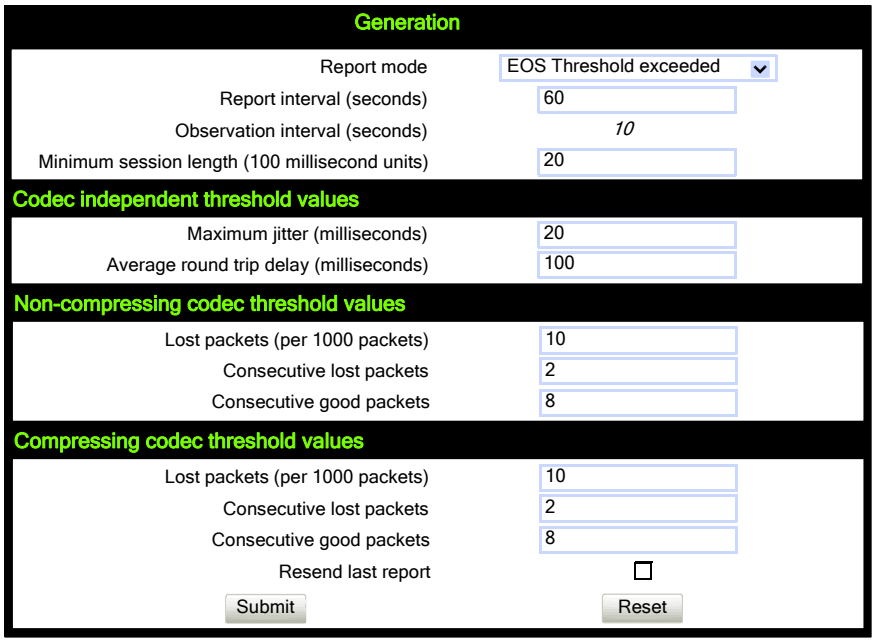
**Non-compressing/ Compressing codecs threshold values:**

- **Lost packets (per 1000 packets)**: When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
  Default: 10
- **Consecutive lost packets**: When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
  Default: 2
- **Consecutive good packets**: When the number of good packets following one another falls below this minimum value, a report is created.
  Default: 8
- **Resend last report**: If checked, the previous report is sent once again on pressing **Sub-Submit**.
  Value range: "Yes", "No"
  Default: "No"

The transmission of report data can be triggered manually by pressing **Send now** in the local menu.

## Administration via WBM

Diagnostics > QoS Reports > Generation



### Administration via Local Phone

- Admin
  - Network
    - QoS
      - Reports
        - Generation
          - **Mode**
          - **Report interval**
          - **Observe interval**
          - **Minimum session length**
        - **Send now**
        - Thresholds
          - **Maximum jitter**
          - **Round-trip delay**
          - Non-compressing:
          - ...**Lost packets (K)**
          - ...**Lost consecutive**
          - ...**Good consecutive**
          - Compressing:
          - ...**Lost packets (K)**
          - ...**Lost consecutive**
          - ...**Good consecutive**

### 3.26.12.2 View Report

OpenStage phones generate QoS reports using a HiPath specific format, QDC (**Q**oS **D**ata **C**ollection). The reports created for the last 6 sessions, i. e. conversations, can be viewed on the WBM.

To enable the generation of reports, please ensure that:

- the switch **QoS traps to QCU** (System > SNMP) is activated (see Section 3.3.9, “SNMP”);
- the conditions for the generation of reports are set adequately (see Section 3.26.12.1, “Conditions and Thresholds for Report Generation”).

For details about QoS reports on OpenScape devices, see the HiPath QoS Data Collection V 1.0 Service Manual.

A QoS report contains the following data:

- **Start of report period - seconds**: NTP time in seconds for the start of the report period.
- **Start of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact start time.
- **End of report period - seconds**: NTP time in seconds for the end of the report period.
- **End of report period - fraction of seconds**: Additional split seconds to be added to the seconds for an exact end time.
- **SNMP specific trap type**: The trap type is a 5 bit value calculated from a list of threshold-exceeding bits. Every time a threshold is exceeded, the associated bit is set, otherwise it is cleared.
  The trace type bits are defined as follows:
  - Bit 0: Jitter threshold was exceeded.
  - Bit 1: Delay threshold was exceeded.
  - Bit 2: Threshold for lost packets was exceeded.
  - Bit 3: Threshold for consecutive lost packets was exceeded.
  - Bit 4: Threshold for consecutive good packets was exceeded.
- **IP address (local)**: IP address of the local phone.
- **Port number (local)**: RTP receiving port of the local phone.
- **IP address (remote)**: IP address of the remote phone that took part in the session.
- **Port number (remote)**: RTP sending port of the local phone.
- **SSRC (receiving)**: RTP Source Synchronization Identifier of the local phone.
- **SSRC (sending)**: RTP Source Synchronization Identifier of the remote phone.
- **Codec**: Number of the Payload Type applied in the session; see RFC 3551 (Table 4 and 5).
- **Maximum packet size**: Maximum size (in ms) of packets received during the report interval.
- **Silence suppression**: Number of silence suppression activation objects found in the RTP stream received. A silence suppression activation object is defined as a period of silence when no encoded voice signals were transmitted by the sender.

- **Count of good packets**: Total amount of good packets.
- **Maximum jitter**: Maximum jitter (in ms) found during the report interval.
- **Maximum inter-arrival jitter**: Maximum of the interarrival jitter values (in ms). The interarrival jitter is the smoothed absolute value of the jitter measurements. It is calculated continuously. For details about the calulation, see RFC 3550.
- **Periods jitter threshold exceeded**: Number of observation intervals in which the threshold for maximum jitter was exceeded.
- **Round trip delay**: Average value of delay calculated for each RTCP packet. The first value is available after about 15 sec.
- **Round trip delay threshold exceeded**: Set to "true" if the average round trip delay threshold value was exceeded in the report interval.
- **Count of lost packets**: Number of packets lost in the course of speech decoding.
- **Count of discarded packets**: Number of the packets discarded without transferring the contents.
- **Periods of lost packets**: Number of observation intervals in which the threshold for lost packets was exceeded.
- **Consecutive packet loss (CPL)**: List of sequences consecutive packets that were all lost, grouped according to the amount of packets per sequence. The first number in the list counts single lost packets, the second number counts sequences of two lost packets, and so on. The last number counts sequences of more than 10 lost packets.
- **Periods of consecutive lost packets**: Number of observation intervals in which the threshold for consecutive lost packets was exceeded.
- **Consecutive good packets (CGP)**: List of sequences consecutive packets that were all processed, grouped according to the amount of packets per sequence. The first number in the list counts single good packets, the second number counts sequences of two good packets, and so on. The last number counts sequences of more than 10 good packets. All values are reset to 0 after an interval without packet loss.
- **Periods of consecutive good packets**: Number of intervals in which the count of lost packets went below the threshold.
- **Count of jitter buffer overruns**: Number of packets rejected because the jitter buffer was full.
- **Count of jitter buffer under-runs**: Increased by one whenever the decoder requests new information on decoding and finds an empty jitter buffer.
- **Codec change on the fly**: The value is 1, if there has been a codec or SSRC change during the observation period, and 0, if there has been no change.
- **Periods with at least one threshold exceeded**: Number of observation intervals with at least one threshold exceedance. If there is no data, the value is 255. The threshold values included are:
  - maximum jitter;
  - lost packets;
  - consecutive lost packets;

    - consecutive good packets.
- **HiPath Switch ID**: Unique number identifying the HiPath switch to which the endpoints are assigned.
- **LTU number**: In HiPath 4000 only, the shelf identification is taken from the shelf containing a gateway.
- **Slot number**: The slot number where the phoneis connected in the shelf.
- **Endpoint type**: Type of the local phone.
- **Version**: Software version of the local phone.
- **Subscriber number type**: Type of subscriber number assigned to the local phone. The possible types are:
    - 1: local number, extension only
    - 2: called number, network call
    - 3: E.164 number of the local phone
- **Subscriber number**: Subscriber number of the local phone.
- **Call ID**: SIP call id.
- **MAC address**: MAC address of the local phone.

## Data viewing via WBM

Diagnostics > QoS reports > View Session Data

**View Session Data**

Select a report to view: QoS Statistics 1

Submit

| | |
|---|---|
| Start of report period - seconds | 2011/10/16 21:51:29 UTC |
| End of report period - seconds | 2011/10/16 21:56:36 UTC |
| SNMP specific trap type | 2 |
| IP address (local) | 192.168.1.235 |
| Port number (local) | 5012 |
| IP address (remote) | 192.168.1.202 |
| Port number (remote) | 5010 |
| SSRC (receiving) | 1481715715 |
| SSRC (sending) | 3244864262 |
| Codec | G.711 PCMU |
| Maximum packet size | 20 |
| Silence suppression | 0 |
| Count of good packets | 15203 |
| Maximum jitter | 2 |
| Maximum inter-arrival jitter | 0 |
| Periods jitter threshold exceeded | 0 |
| Round trip delay | 433 |
| Round trip delay threshold exceeded | ☐ |
| Count of lost packets | 0 |
| Count of discarded packets | 0 |
| Periods of lost packets | 0 |
| Consecutive packet loss (CPL) | 255,255,255,255,255,255,255,255,255,255 |
| Periods of consecutive lost packets | 255 |
| Consecutive good packets (CGP) | 255,255,255,255,255,255,255,255,255,255 |
| Periods of consecutive good packets | 255 |
| Count of jitter buffer overruns | 0 |
| Count of jitter buffer under-runs | 0 |
| Codec change on the fly | |
| Periods with at least one threshold exceeded | 0 |
| HiPath Switch ID | Asterisk PBX 1.6.2.19 |
| LTU number | 255 |
| Slot number | 255 |
| Endpoint type | OpenStage 80 |
| Version | V3 R0.50.0 SIP 110924 |
| Subscriber number type | 0 |
| Subscriber number | 3339 |
| Call ID | 05b4445aeaf00008 |
| MAC address | 0001e325eaca |

## 3.26.13 Core dump

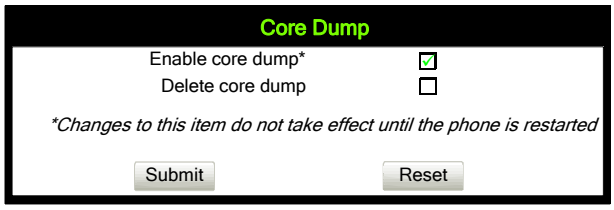
If **Enable core dump** is checked, a core dump will be initiated in case of a severe error. The core dump will be saved to a file. By default, this function is activated.

If **Delete core dump** is activated, the current core dump file is deleted on **Submit**. By default, this is not activated.

If one or more core dump file exist, hyperlinks for downloading will be created automatically.

### Administration via WBM

Diagnostics > Miscellaneous > Core Dump



## 3.26.14 Remote Tracing – Syslog

All trace messages created by the components of the phone software can be sent to a remote server using the syslog protocol. This is helpful especially for long-term observations with a greater number of phones.

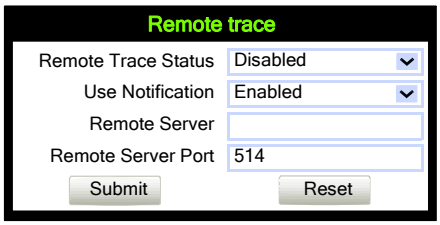
To enable remote tracing, **Remote trace status** must be set to "Enabled". Furthermore, the IP address of the server receiving the syslog messages must be entered in **Remote ip**, and the corresponding server port must be given in **Remote port**.

With version V2, the **User notification** parameter controls whether the user is notified about the remote tracing or not. If user notification is enabled, a blinking symbol ( on OpenStage 60/80; on OpenStage 15/20/40) will inform the user when remote tracing is active, that is, when **Remote trace status** is set to "Enabled".

### Administration via Local Phone

- Admin
  - Maintenance
    - Remote trace
      - **Remote trace status**
      - **User notification**
      - **Remote ip**
      - **Remote port**

### Administration via WBM



## 3.26.15 HPT Interface (For Service Staff)

For special diagnosis and maintenance tasks, the service staff may employ the HPT tool, which is able to control and observe an OpenStage phone remotely. For security reasons, this tool can only be used when a dongle key file is uploaded to the phone (see Section 3.16.10, “Dongle Key”). This key is accessable to the service staff only. It is specific for a particular SIP firmware version, but it will also be valid for previous versions.

There are 2 types of HPT sessions, control session and observation session.

A control session allows for activating phone functions remotely. When a control session is established, the following changes will occur:

- The display shows a message indicating that remote service is active.
- Handset, microphone, speaker, headset, and microphone are disabled.

An observation session allows for supervising events on the phone, like, for instance, pressing a key, incoming calls or navigating in the menus. Before an observation session is started, the user is prompted for allowing the observation. During an observation session, the phone operates normally, including loudspeaker, microphone and ringer. Thus, the local user can demonstrate an error towards the service staff that is connected via HPT.

The HPT interface is enabled by downloading the dongle key file to the phone (see Section 3.16.10, “Dongle Key”). It can be disabled via local menu or WBM. Thereby, the dongle key file is deleted. To enable the HPT interface again, the file must be downloaded anew.

The session data is written to a log file on the phone. It can be downloaded from the Diagnostics > Fault trace configuration menu (see Section 3.26.9, “Fault Trace Configuration”).

### Administration via WBM (Disable)

Maintenance > HPT interface

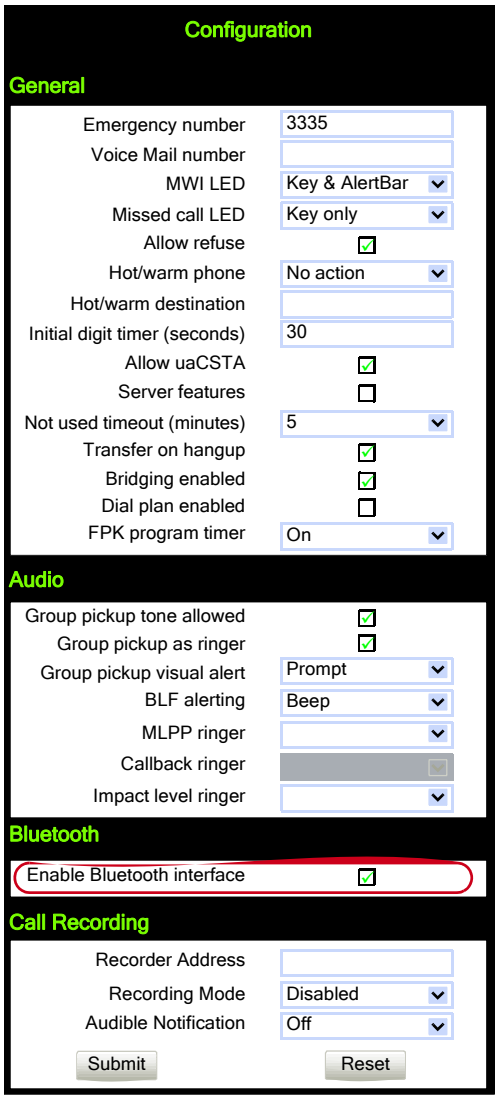
## 3.27 Bluetooth (OpenStage 60/80)

The Bluetooth interface can be enabled or disabled in the admin menu. By default, it is enabled. If Bluetooth is enabled, the user has the possibility to activate or deactivate it via the user menu.

This parameter can also be configured under System > Features > Feature access > Bluetooth (see Section 3.7, “Feature Configuration”) or Bluetooth > Enable Bluetooth interface.

### Administration via WBM

System > Features > Configuration



### Administration via Local Phone

Bluetooth can be enabled or disabled via the local admin menu:

```
└── Admin
    └── System
        └── Features
            └── Configuration
                └── Bluetooth
                    └── Enable
```

or

```
└── Admin
    └── System
        └── Features
            └── Feature Access
                └── Services
                    └── Bluetooth
                        ├── Allow
                        └── Disallow
```

## 3.28 MWI LED

This configurable item is added to the Administrator settings to allow the Administrator to control how new VoiceMails are indicated to the user; via the "Envelope" mode key LED only, via the Top LED only or via both LEDs.

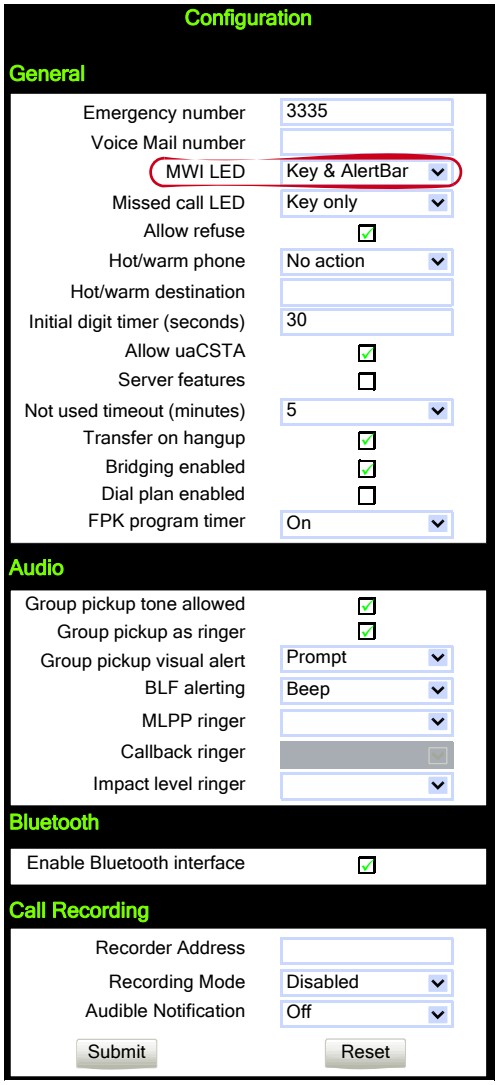
The selection field offers the choice between:

- "Key only" (default)
- "Key & AlertBar"
- "AlertBar only"

Default setting for **OpenStage 40 US** is "**AlertBar only**". After a factory reset, the system will be reset to this value.

### Administration via WBM

System > Features > Configuration



## Administration via Local Phone

- Admin
  - System
    - Features
      - Configuration
        - **MWI LED**

## 3.29 Missed Call LED

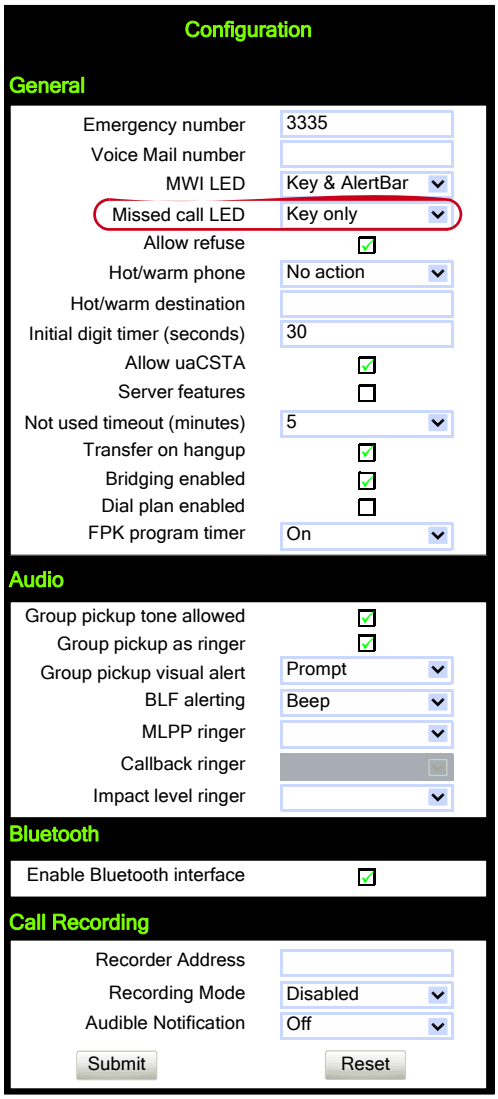
This configurable item is added to the Administrator settings to allow the Administrator to control how new Missed Calls are indicated to the user; via the "Envelope" mode key LED only, via the Top LED only, via both LEDs or no LED.

The selection field offers the choice between:

- "Key only" (default)
- "Key & AlertBar"
- "AlertBar only"
- "No LED"

### Administration via WBM

System > Features > Configuration



**Administration via Local Phone**

```
└--- Admin
     └--- System
          └--- Features
               └--- Configuration
                    └--- Missed call LED
```

## 3.30 Impact Level Notification

Communications for the Public Sector Network (PSN) is seen as originating from or terminating to zones with differing 'impact' levels (the impact level indicates how the phone user should handle the call conversation). The purpose is to notify the OpenStage phone users when they are connecting or in a call where another party in the call is in a lower Impact Level (IL) zone.

This feature uses a UI mechanism to notify/remind the phone user that the call may require special treatment. This involves special icons, text indications, and special audio (ringer or tone as appropriate). There are no restrictions on call handling as a result of any special status for the call.

Thus the Impact Level Notification feature only involves UI changes that are triggered by receiving new SIP headers and affects the following:

- Prompts presented to alert for incoming calls
- Prompts presented to monitor progress for outgoing calls
- Connected call displays
- Call scenarios involving multiple calls
- Retrieving a held call

However, since there are no call restrictions explicit for the Impact Level Notification feature the solution needs to consider some additional scenarios:

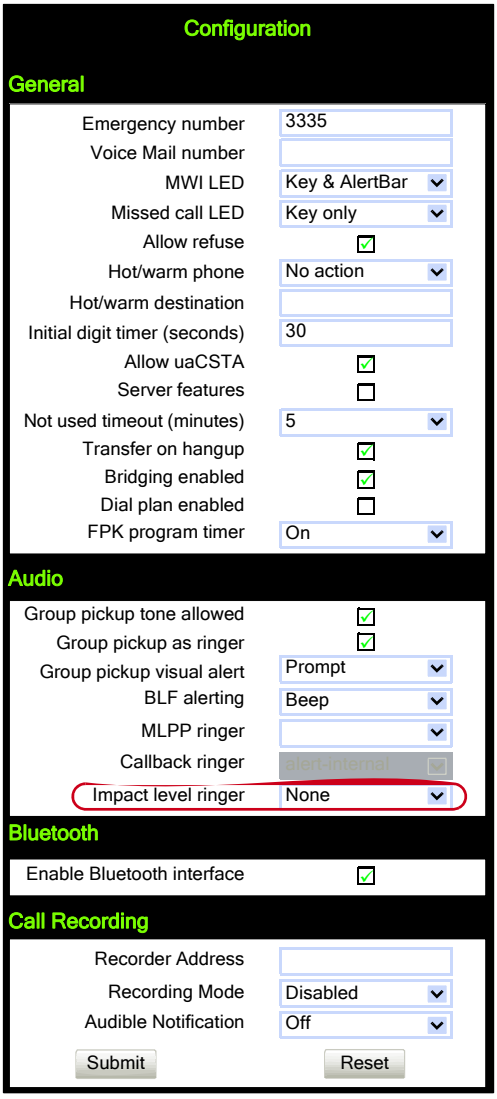
- Group pickup
- Directed pickup
- Callback
- CTI action
- Shared lines on a Keyset

This feature cannot be turned off at the phone since it is driven solely by the OSV.

The OSV is responsible for being aware of the impact level of the phone (the phone does not have control of its own level) and the impact levels of all other endpoints that are participating in a call with the phone. The OSV uses this information to signal (via a new SIP header) the phone when the call is to be treated as from a lower impact level. It does this during the start of a call or anytime during a call.

### Data required

- **Impact level ringer**: Identifies one of the named distinctive ringers to be used in place of the normal ringer for calls from a lower impact level.
  Value range: the offered values are those definded in "Ringer Settings" > Distinctive", e.g. "Bellcore-dr1" or any arbitrary name




The phone plays the configured Impact Level Notification ringer when the call is from a lower impact level. The ringer has to be configured in the ringer setting table (see Section 3.14, “Ringer Setting”).

### Administration via Local Phone

- Admin
  - System
    - Features
      - Configuration
        - Audio
          - **Lower IL ringer**

# 4 Technical Reference

## 4.1 Menus

This section describes the structure of the administration menus of the OpenStage phone. For information on user menus, please refer to the user manual.

### 4.1.1 Web Interface Menu

#### 4.1.1.1 Menu Structure

Admin Login

**Applications** (OpenStage 60/80)

- **XML applications**
  - Add application
  - Modify/Delete application
  - Xpressions
  - Add messages application
  - Add messages applicationAdd phonebook application
  - Add call log application
  - Add help application

Bluetooth

**Network**

- General IP configuration
- IPv4 configuration
- IPv6 configuration
- Update Service (DLS)
- QoS
- Port configuration
- LLDP-MED operation

**System**

- System Identity
- SIP interface
- Registration
- SNMP
- **Features**

- Configuration
- DSS settings
- Program keys > Line (V2 on OpenStage 15/40/60/80)
- Key Module 1
- Key Module 2
- Fixed keys
- Keyset operation
- Addressing
- Call completion
- Feature access

**Security**

- System
- SDES Config
- Access control
- Logging
- Faults

**File transfer**

- Defaults
- Phone application
- Hold music
- Picture Clip (OpenStage 60/80)
- LDAP (OpenStage 60/80)
- Logo (OpenStage 40/60/80)
- Screensaver (OpenStage 60/80)
- Ringer file
- Dongle key

**Local functions**

- Directory settings
- Messages settings

**Locality**

- Canonical dial settings
- Canonical dial lookup
- Canonical dial
- Phone location

- Energy saving
- Call logging

Date and time

**Speech**
- Codec preferences
- Audio settingsAudio settings

General information

**Security and Policies**
- **Password**
  - Generic policy
  - Admin policy
  - User policy
  - Character set
  - Change Admin password
  - Change User password
- **Certificates**
  - Generic
  - Authentication policy

**Ringer Setting**
- Distinctive
- Map To Specials

Mobility

**Diagnostics**
- **Diagnostic information**
  - View
  - User acess
- LLDP-MED TLVs
- Fault trace configuration
- **EasyTrace Profiles**
  - Bluetooth handsfree profile (OpenStage 60/80)
  - Bluetooth headset profile (OpenStage 60/80)
  - Call connection
  - Call log problems
  - Call Recording
  - DAS connection
  - DLS data errors
  - Help application problems
  - Key input problems
  - LAN connectivity problems
  - Messaging application problems

- Mobility problems
- Phone administration problems
- Phonebook (LDAP) problems (OpenStage 60/80)
- Phonebook (local) problems (OpenStage 60/80)
- Server based application problems (OpenStage 60/80)
- Sidecar problems
- SIP standard multiline
- SIP standard singleline
- Speech problems
- Tone problems
- USB backup/restore
- Voice recognition problems (OpenStage 60/80)
- Web based management
- 802.1x problems
- Clear all profiles

Bluetooth Advanced Traces

**QoS Reports**

- Generation
- View Session Data

**Miscellaneous**

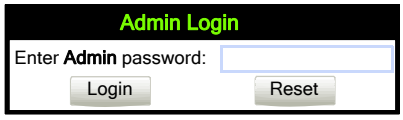
- IP tests
- Memory information
- Core Dump

**Maintenance**

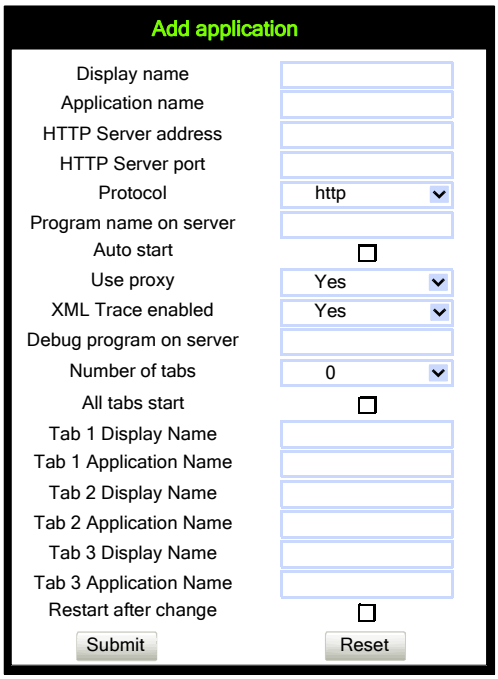
Remote trace
Restart Phone
Factory reset
HPT interface
Secure Shell
Diagnostic call

### 4.1.1.2 Web Pages

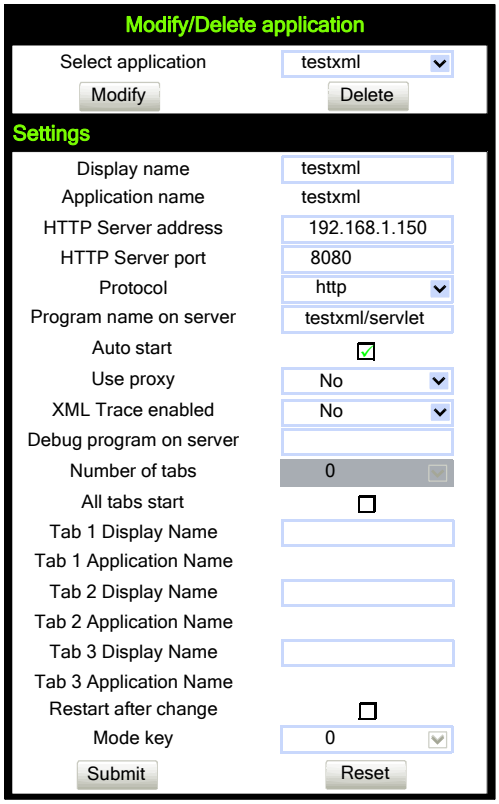
## Admin Login



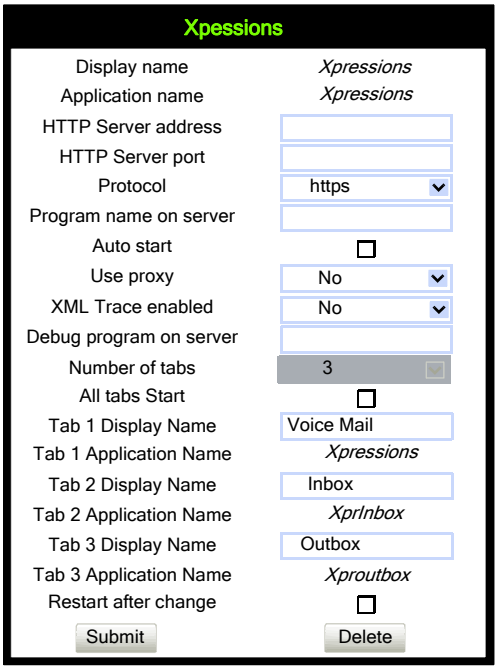

## Add application



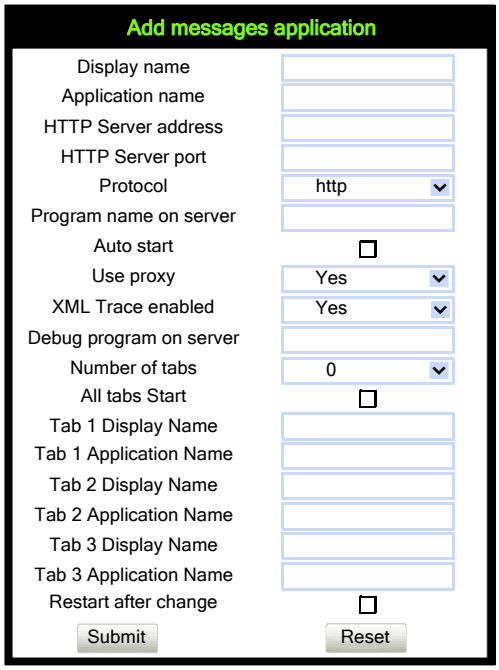
## Modify/Delete application



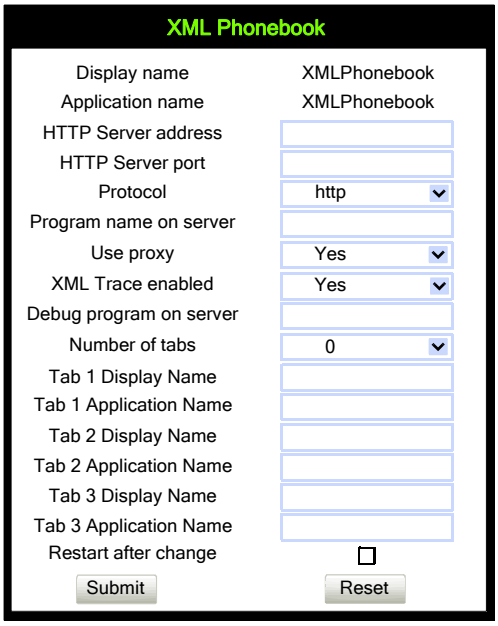

## Xpressions



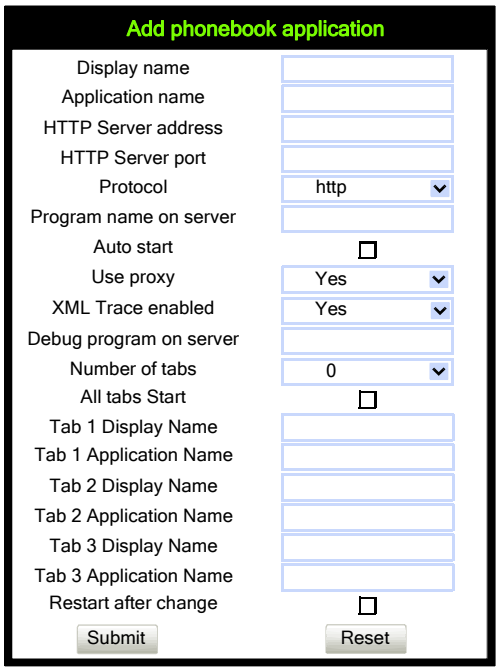
## Add messages application



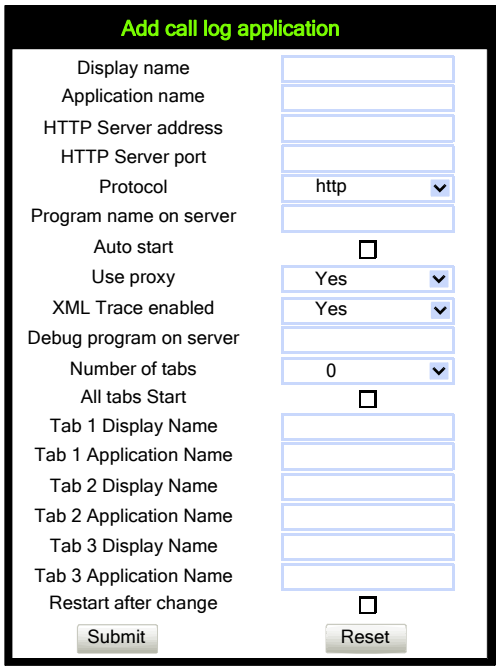

## XML Phonebook (up to V2R0)



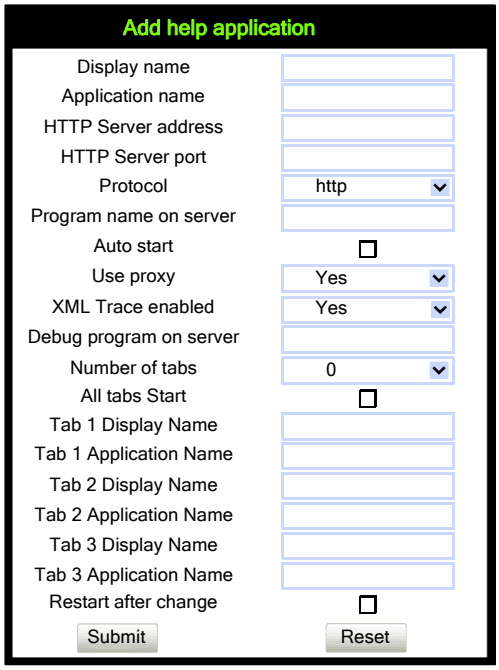
## Add phonebook application



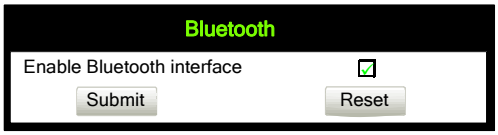

## Add call log application



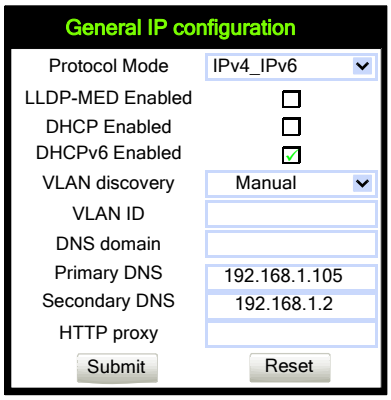
## Add help application



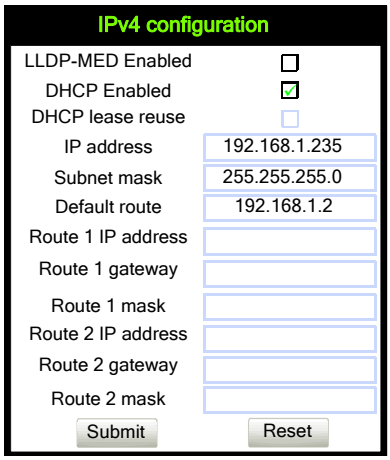

## Bluetooth



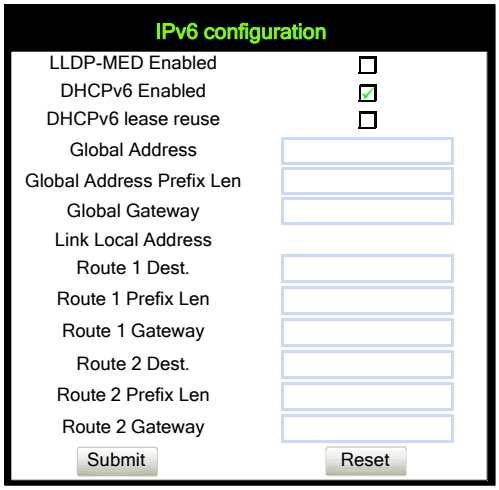

## General IP configuration



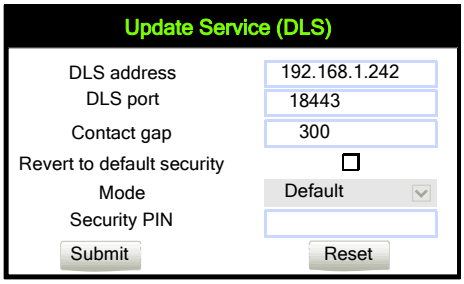
## IPv4 configuration



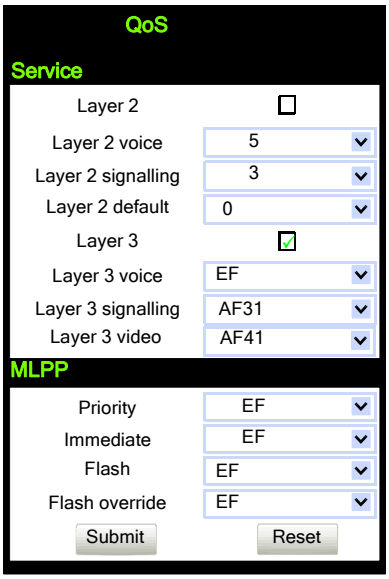

## IPv6 configuration



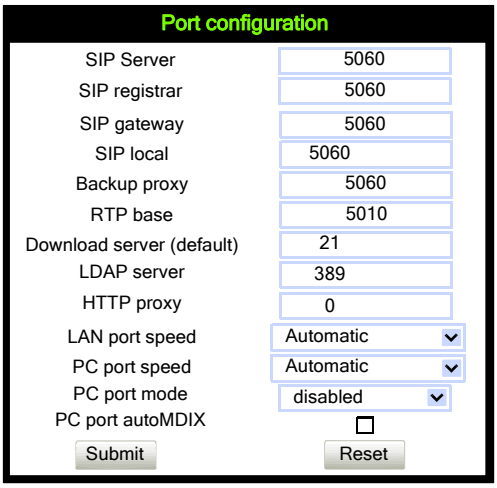

## Update Service (DLS)



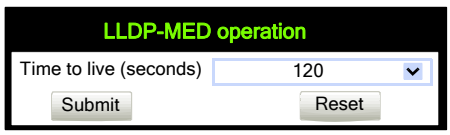
## QoS



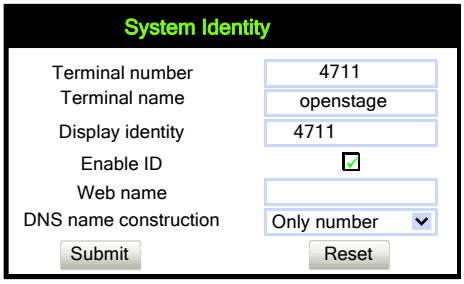

## Port configuration



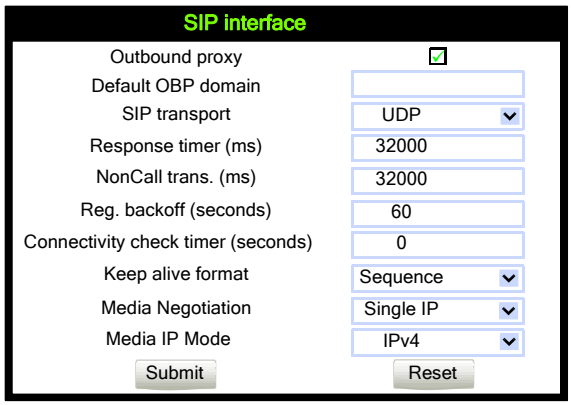

## LLDP-MED operation



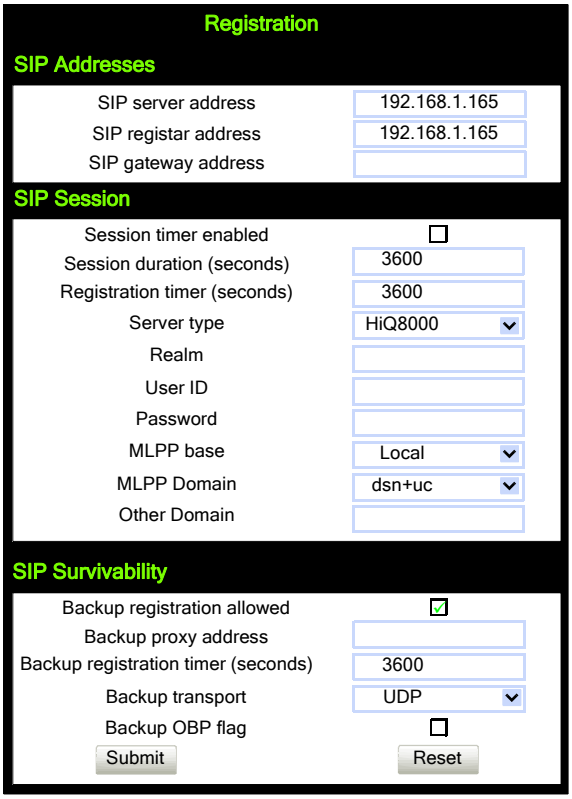
## System Identity



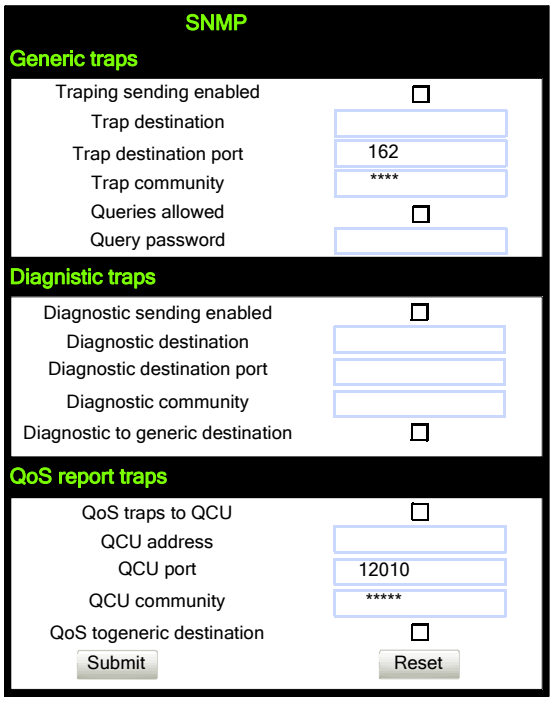

## SIP interface



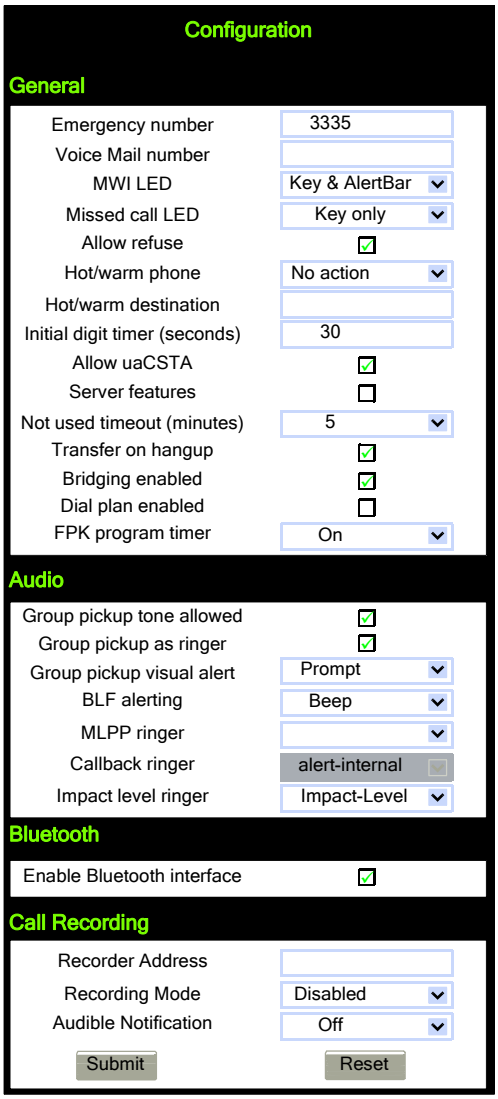
## Registration



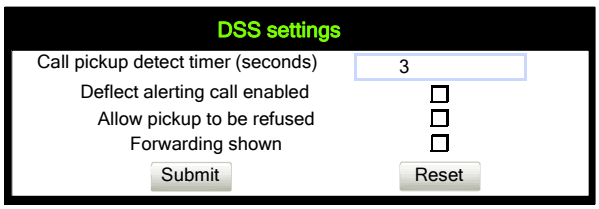
## SNMP


SNMP
Generic traps
Traping sending enabled
Trap destination
Trap destination port
162
Trap community
****
Queries allowed
Query password
Diagnistic traps
Diagnostic sending enabled
Diagnostic destination
Diagnostic destination port
Diagnostic community
Diagnostic to generic destination
QoS report traps
QoS traps to QCU
QCU address
QCU port
12010
QCU community
*****
QoS togeneric destination
Submit
Reset

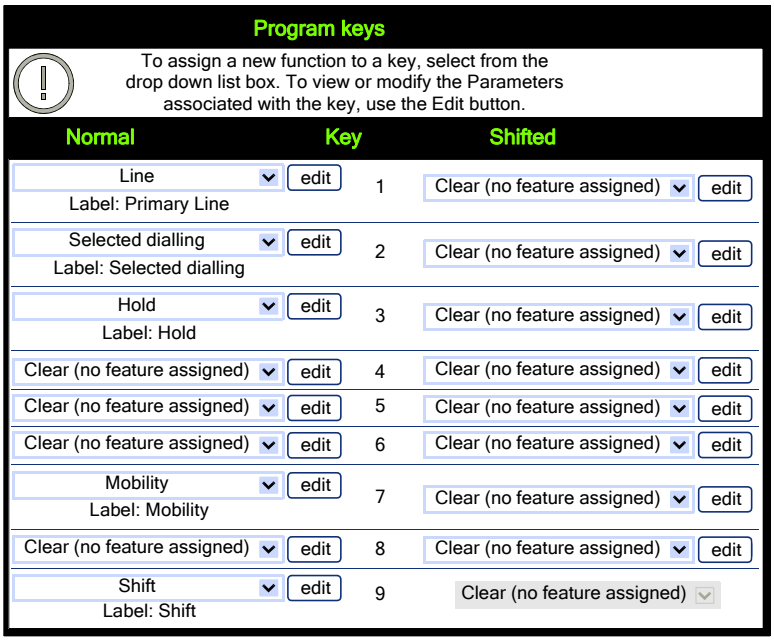
## Configuration



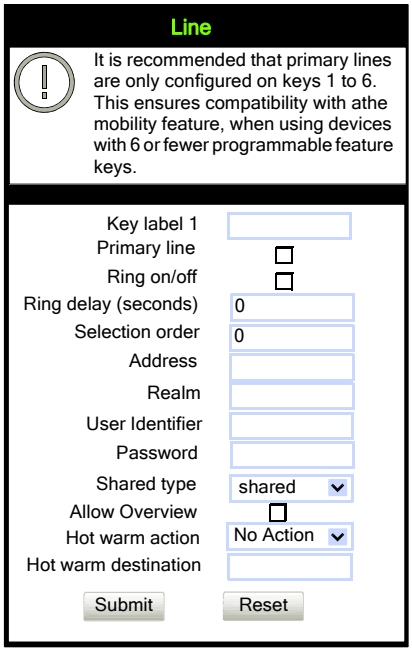

## DSS settings



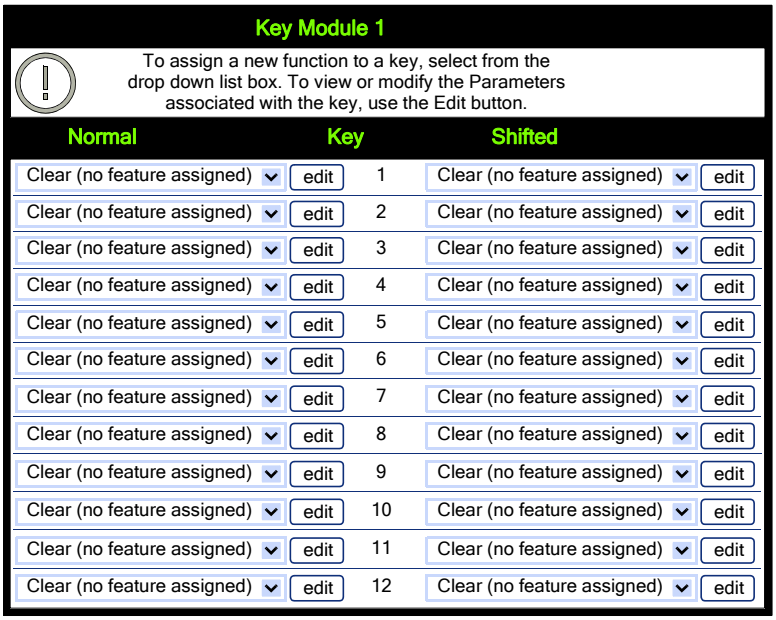
## Program keys



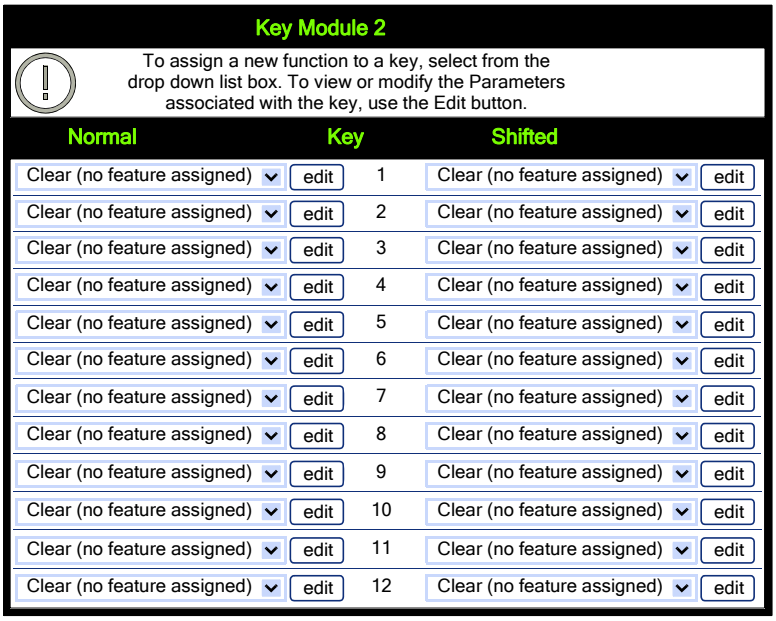

## Line (V2 on OpenStage 15/40/60/80)



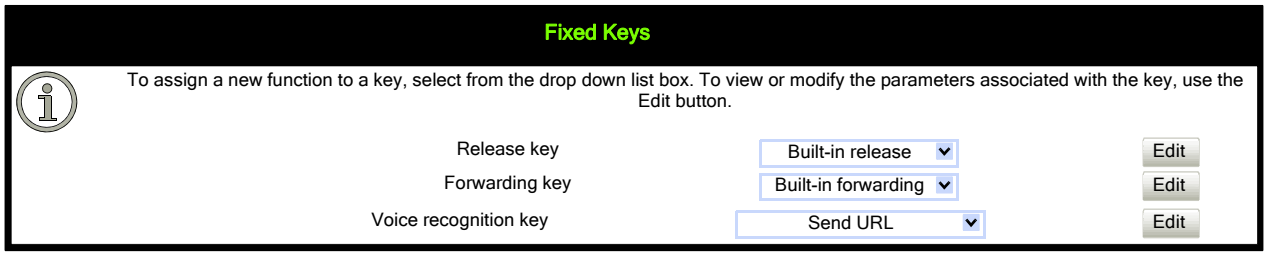
## Key Module 1



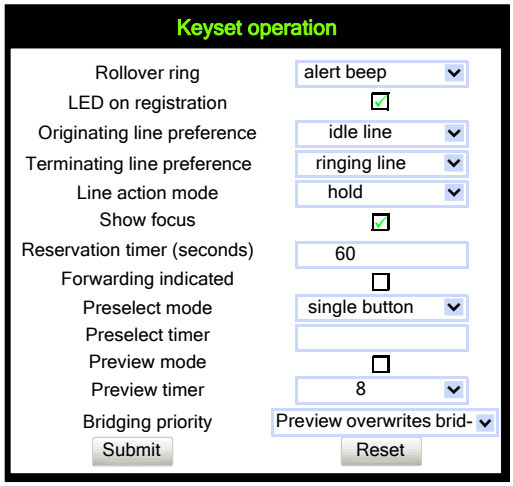

## Key Module 2



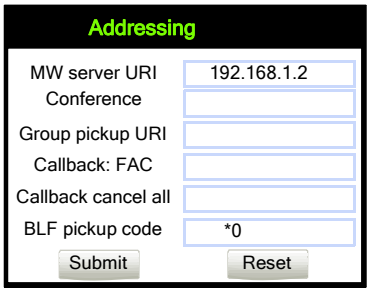
## Fixed keys


Fixed Keys
To assign a new function to a key, select from the drop down list box. To view or modify the parameters associated with the key, use the Edit button.
Release key
Built-in release
Edit
Forwarding key
Built-in forwarding
Edit
Voice recognition key
Send URL
Edit

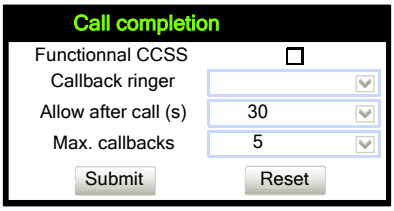
## Keyset operation



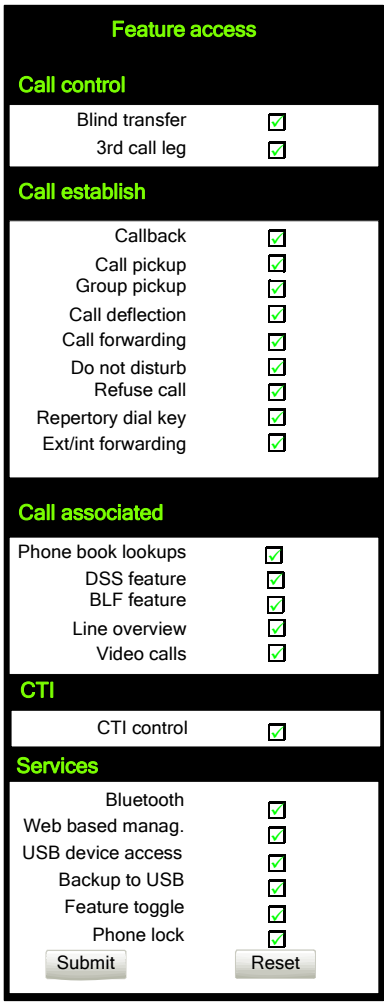

## Addressing



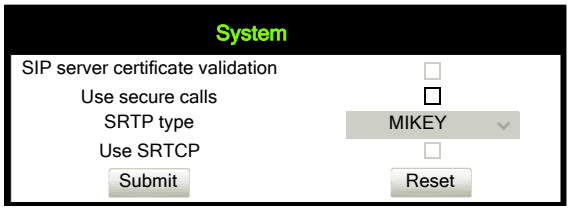
## Call completion



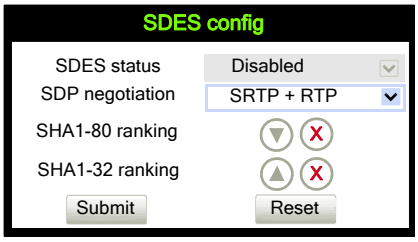

## Feature access



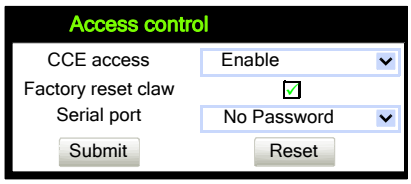
## System



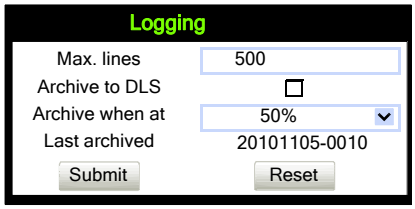

## SDES Config



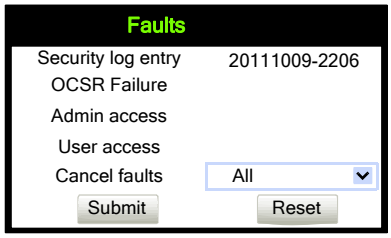

## Access control



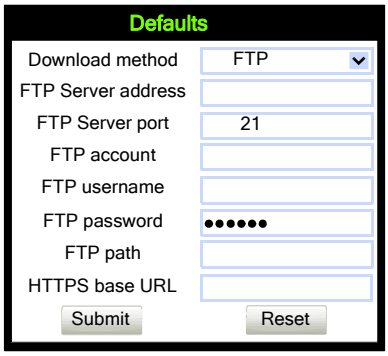

## Logging



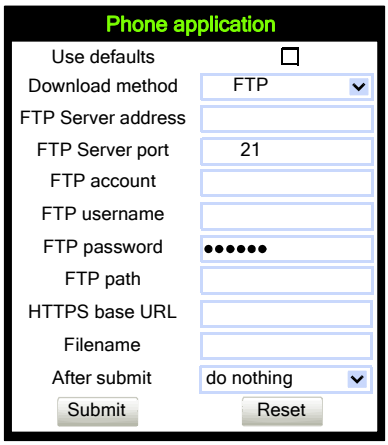

## Faults



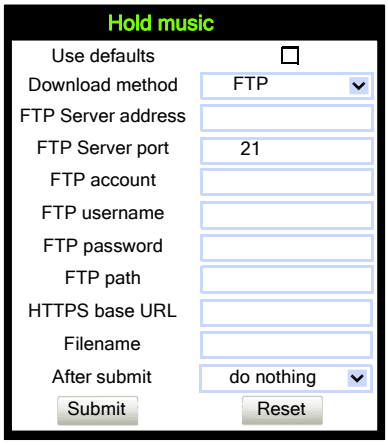
## Defaults



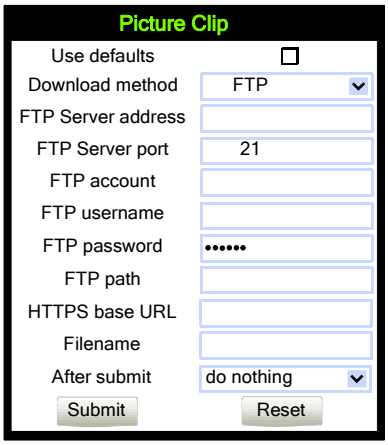

## Phone application



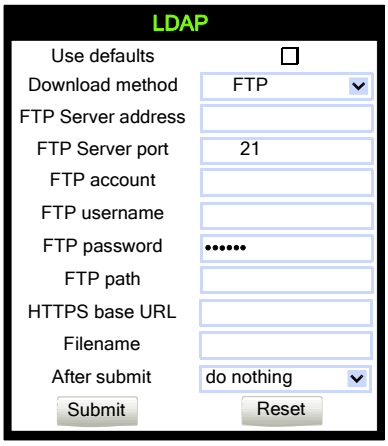

## Hold music



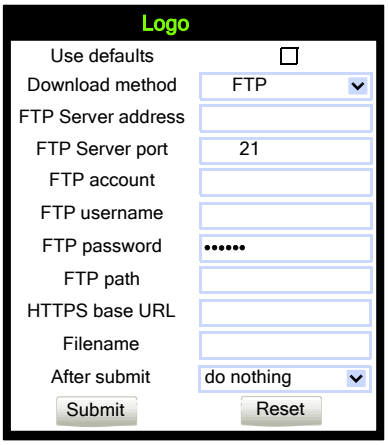
## Picture Clip



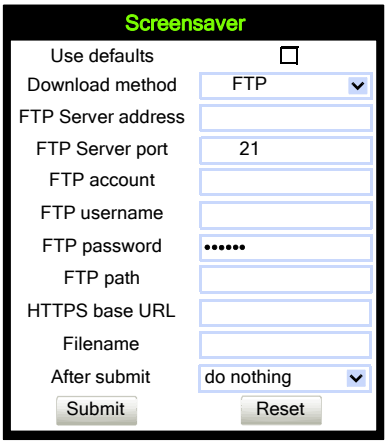

## LDAP



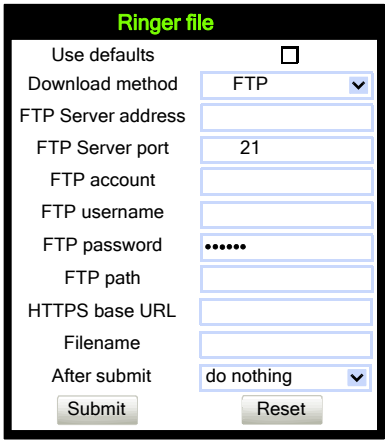
## Logo



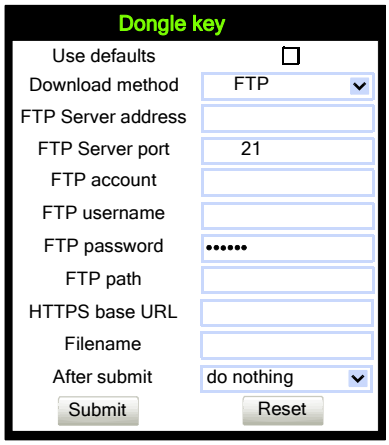

## Screensaver



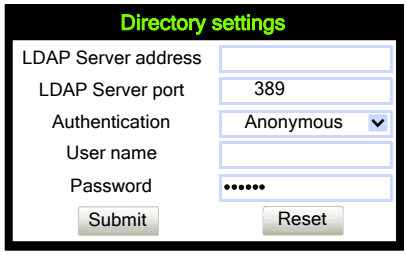
## Ringer file



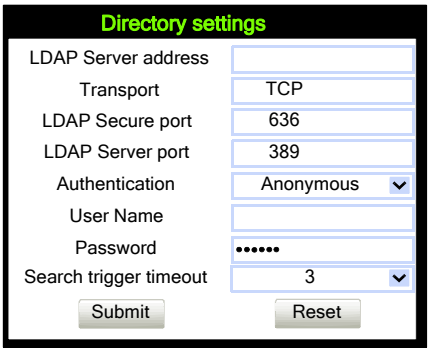

## Dongle key



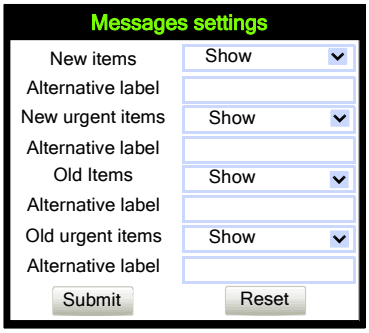

## Directory settings (OpenStage 40/20/15 )



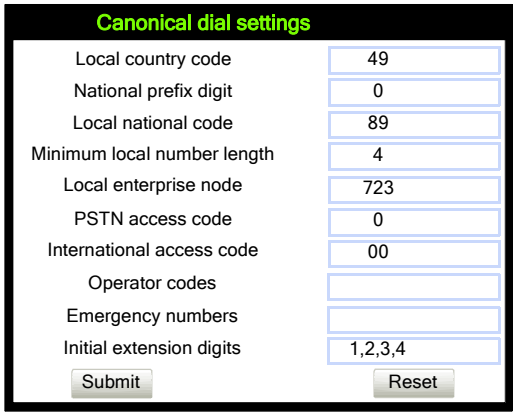
## Directory settings



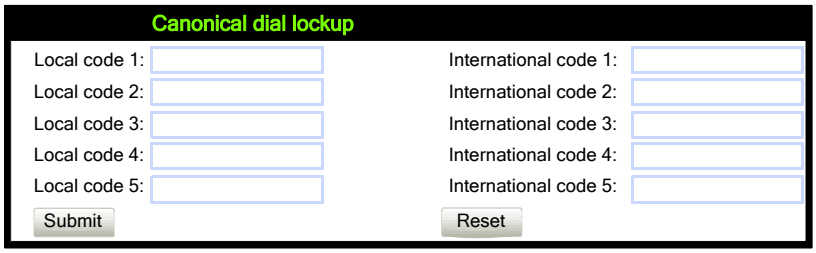

## Messages settings



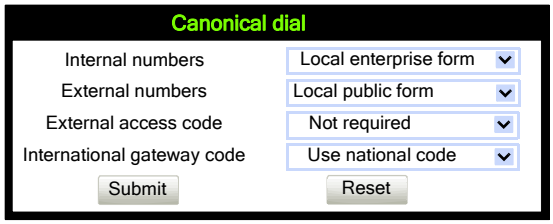

## Canonical dial settings



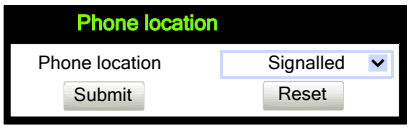
## Canonical dial lookup




## Canonical dial



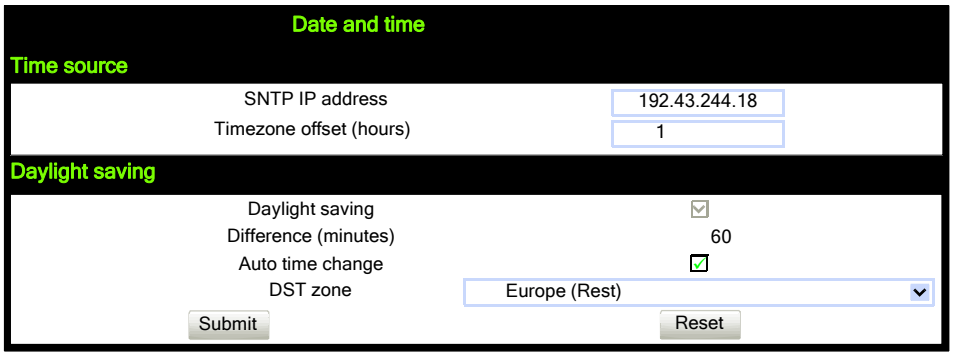

## Phone location



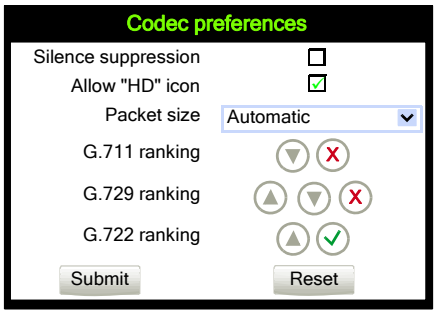

## Energy saving

## Call logging

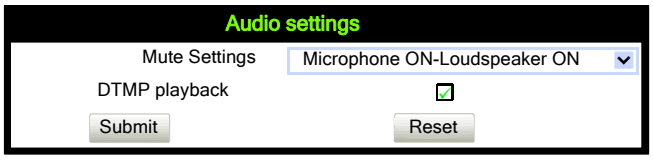
## Date and time



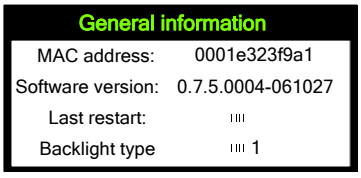

## Codec preferences



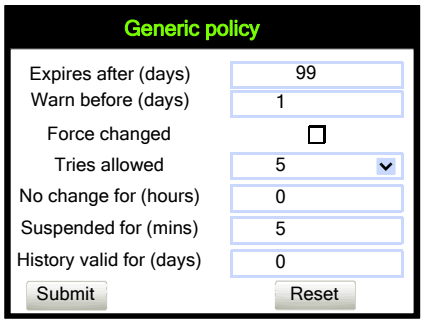

## Audio settings



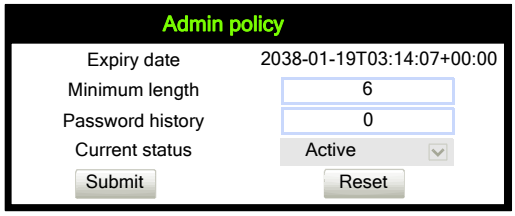

## General information



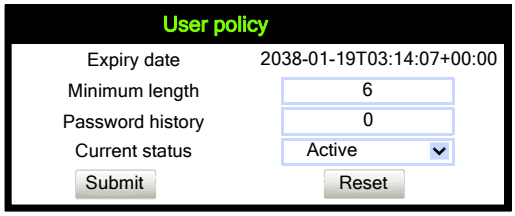
## Generic policy



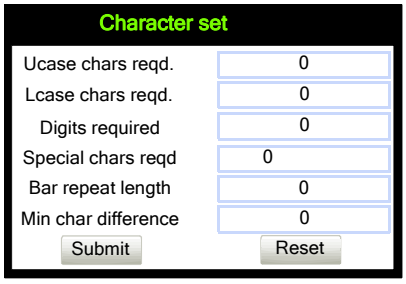

## Admin policy



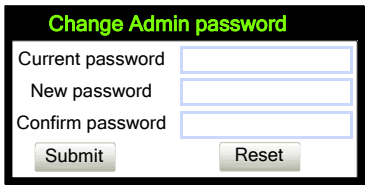

## User policy



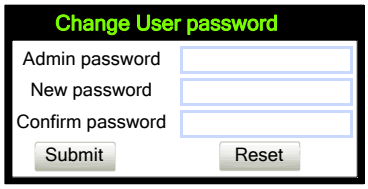

## Character set



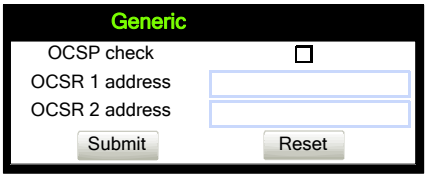
## Change Admin password



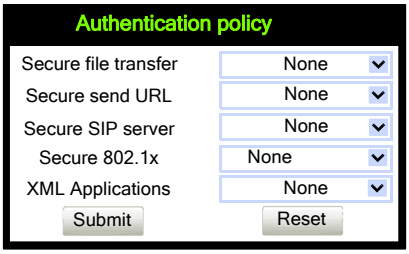

## Change User password



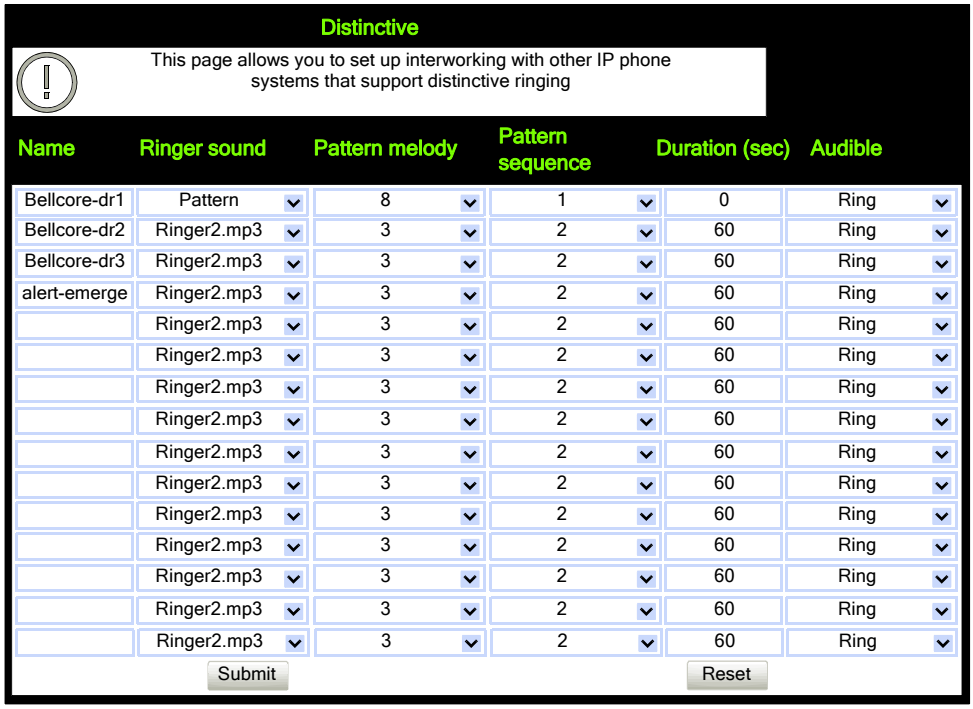

## Generic



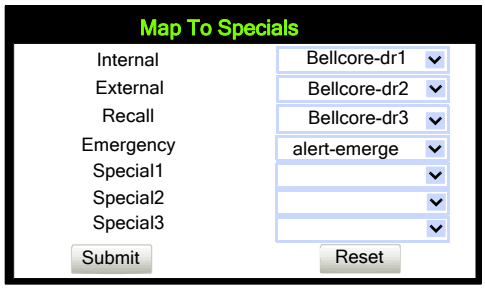

## Authentication policy



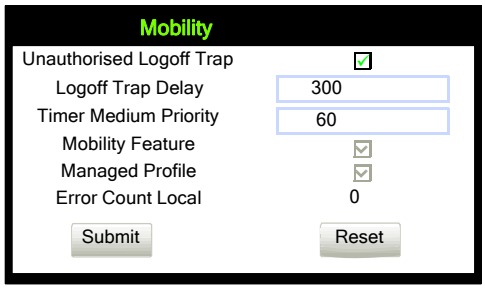
## Distinctive



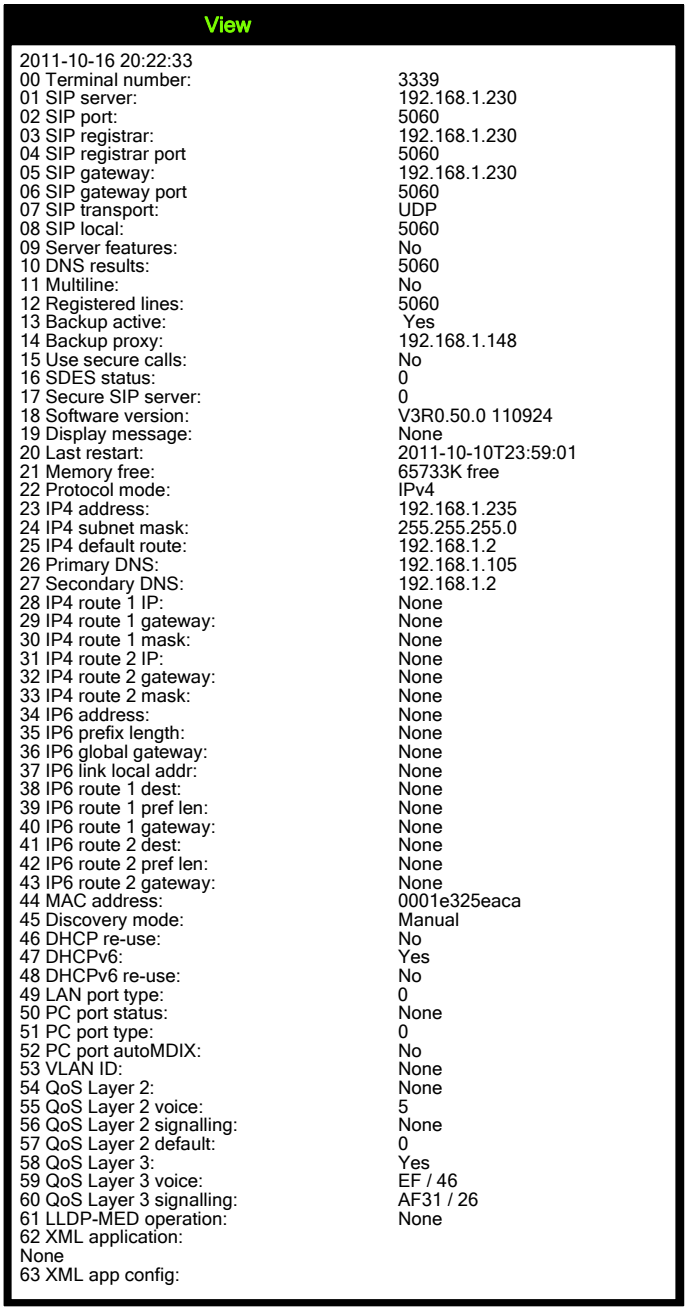

## Map To Specials




## Mobility

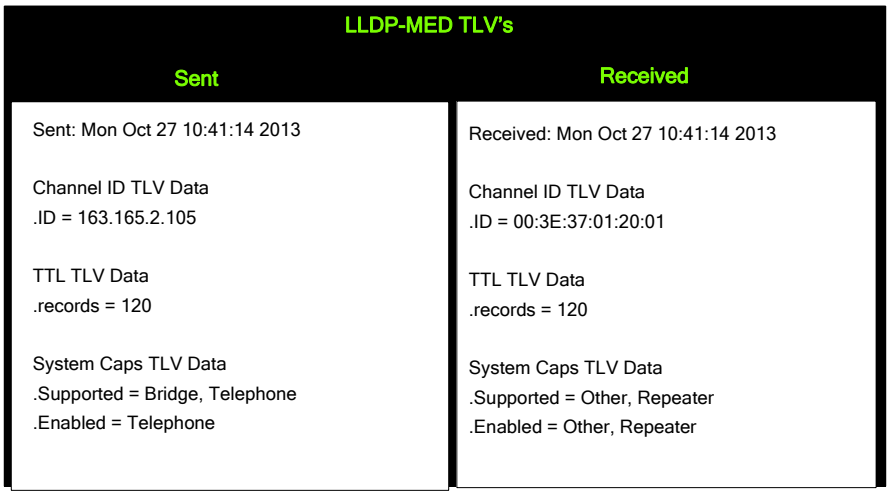


## View

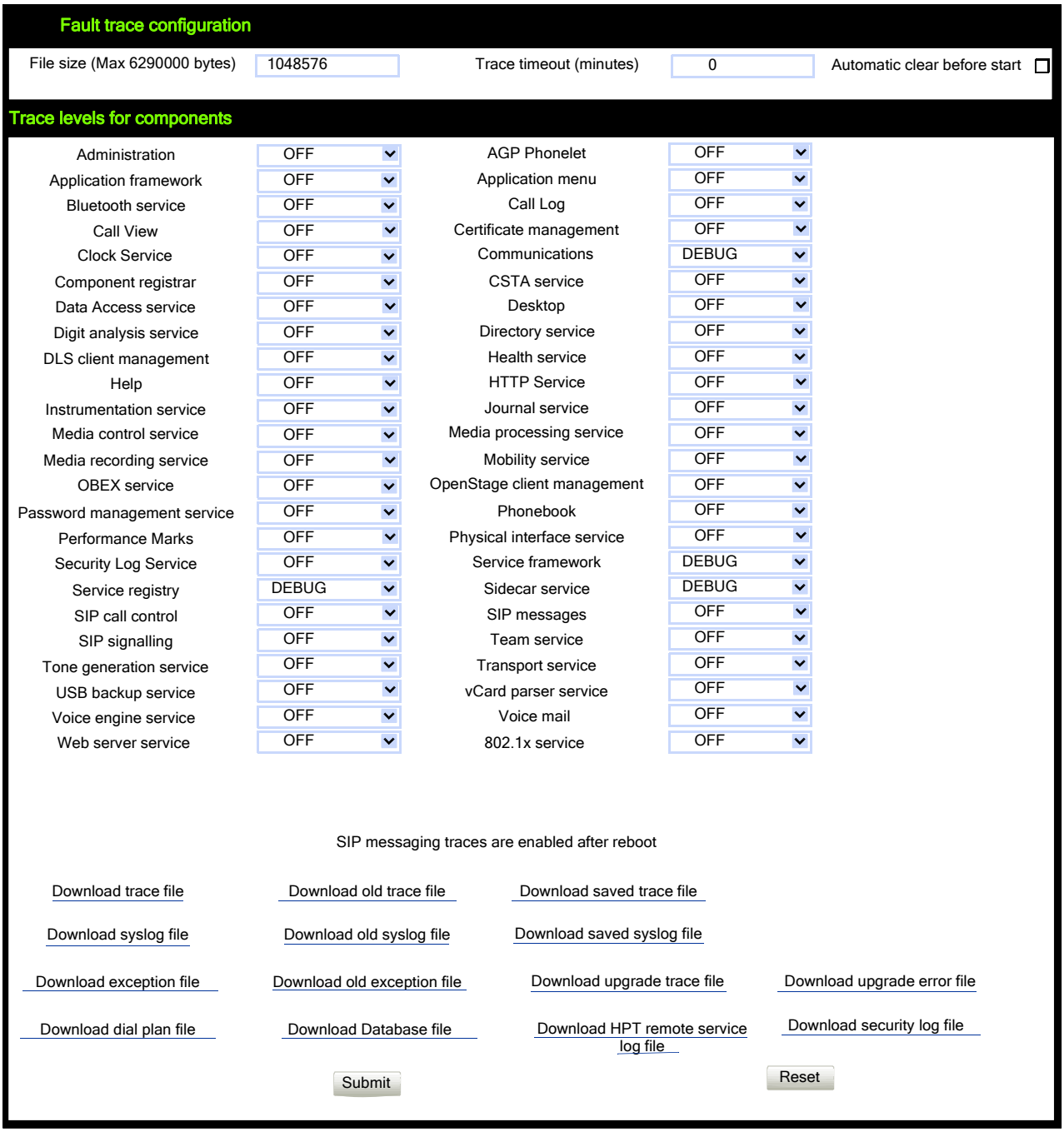

View
2011-10-16 20:22:33
00 Terminal number: 3339
01 SIP server: 192.168.1.230
02 SIP port: 5060
03 SIP registrar: 192.168.1.230
04 SIP registrar port 5060
05 SIP gateway: 192.168.1.230
06 SIP gateway port 5060
07 SIP transport: UDP
08 SIP local: 5060
09 Server features: No
10 DNS results: 5060
11 Multiline: No
12 Registered lines: 5060
13 Backup active: Yes
14 Backup proxy: 192.168.1.148
15 Use secure calls: No
16 SDES status: 0
17 Secure SIP server: 0
18 Software version: V3R0.50.0 110924
19 Display message: None
20 Last restart: 2011-10-10T23:59:01
21 Memory free: 65733K free
22 Protocol mode: IPv4
23 IP4 address: 192.168.1.235
24 IP4 subnet mask: 255.255.255.0
25 IP4 default route: 192.168.1.2
26 Primary DNS: 192.168.1.105
27 Secondary DNS: 192.168.1.2
28 IP4 route 1 IP: None
29 IP4 route 1 gateway: None
30 IP4 route 1 mask: None
31 IP4 route 2 IP: None
32 IP4 route 2 gateway: None
33 IP4 route 2 mask: None
34 IP6 address: None
35 IP6 prefix length: None
36 IP6 global gateway: None
37 IP6 link local addr: None
38 IP6 route 1 dest: None
39 IP6 route 1 pref len: None
40 IP6 route 1 gateway: None
41 IP6 route 2 dest: None
42 IP6 route 2 pref len: None
43 IP6 route 2 gateway: None
44 MAC address: 0001e325eaca
45 Discovery mode: Manual
46 DHCP re-use: No
47 DHCPv6: Yes
48 DHCPv6 re-use: No
49 LAN port type: 0
50 PC port status: None
51 PC port type: 0
52 PC port autoMDIX: No
53 VLAN ID: None
54 QoS Layer 2: None
55 QoS Layer 2 voice: 5
56 QoS Layer 2 signalling: None
57 QoS Layer 2 default: 0
58 QoS Layer 3: Yes
59 QoS Layer 3 voice: EF / 46
60 QoS Layer 3 signalling: AF31 / 26
61 LLDP-MED operation: None
62 XML application:
None
63 XML app config:

## User acess

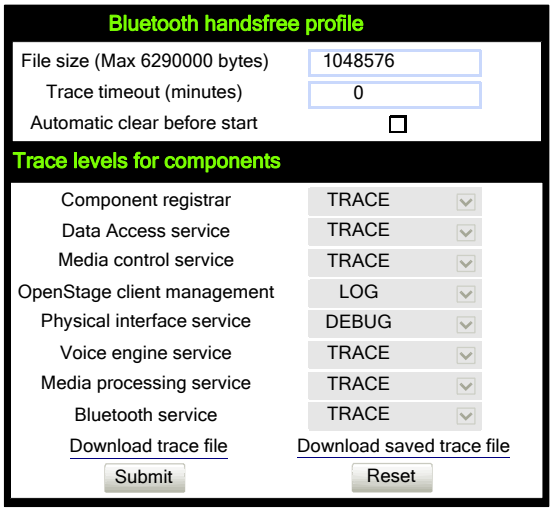
## LLDP-MED TLVs



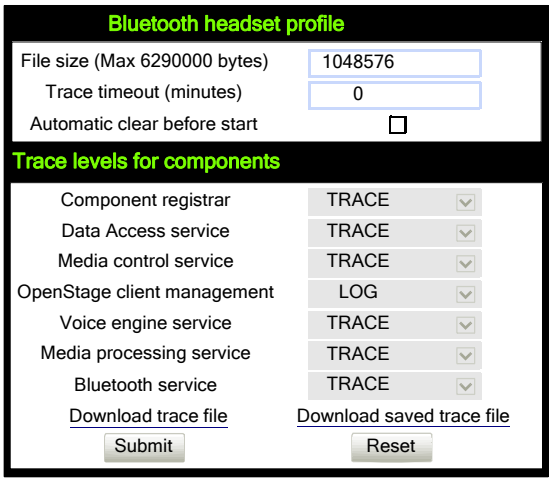
## Fault trace configuration



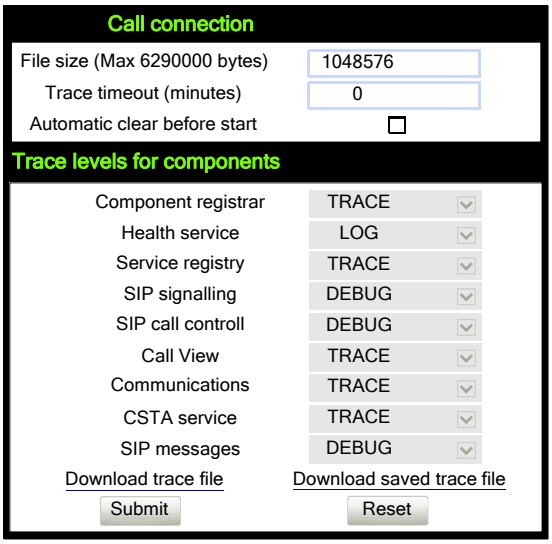
## Bluetooth handsfree profile



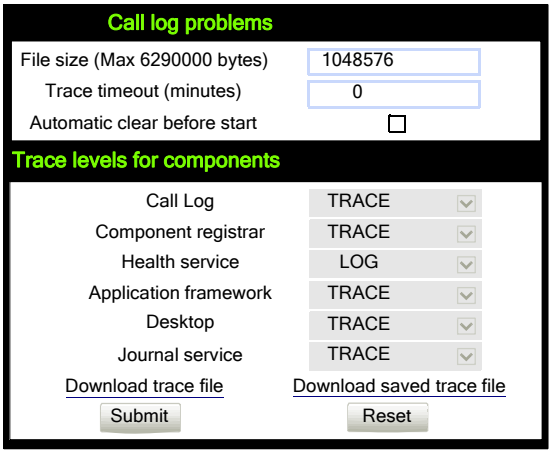

## Bluetooth headset profile



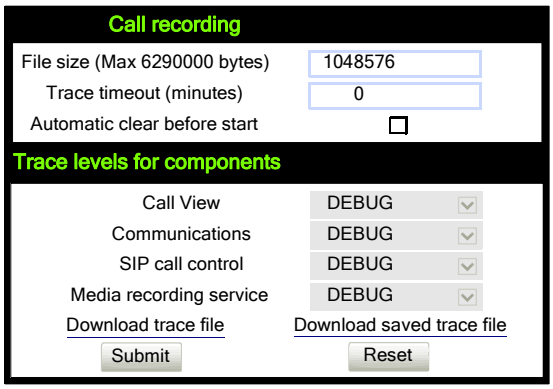
## Call connection



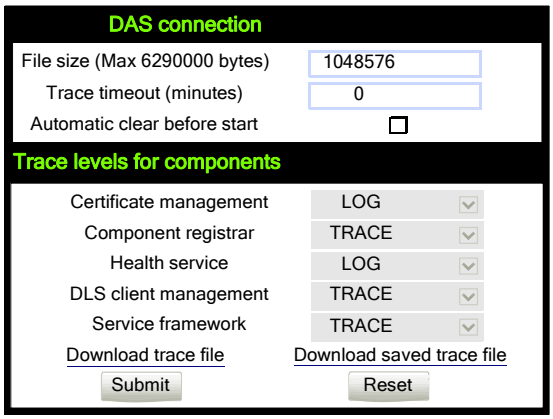

## Call log problems



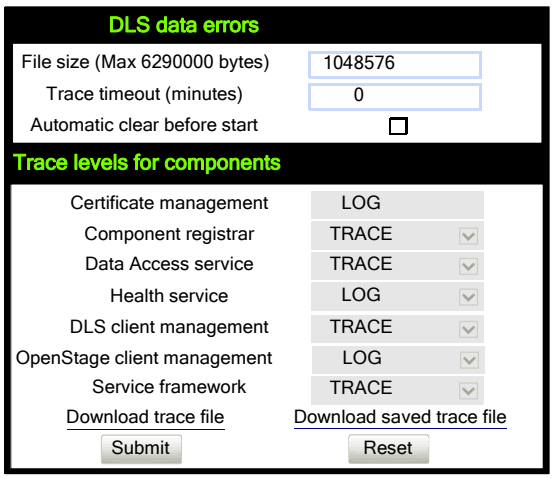
## Call Recording



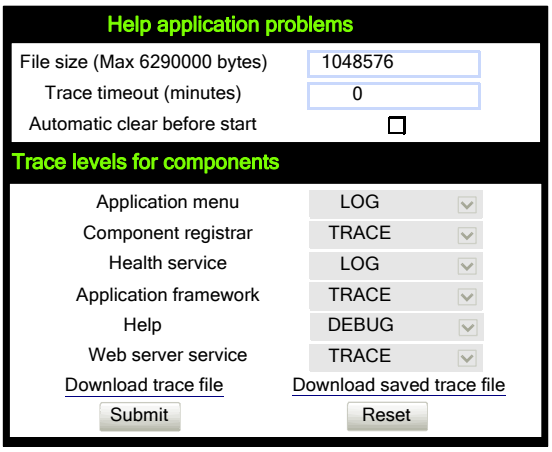

## DAS connection



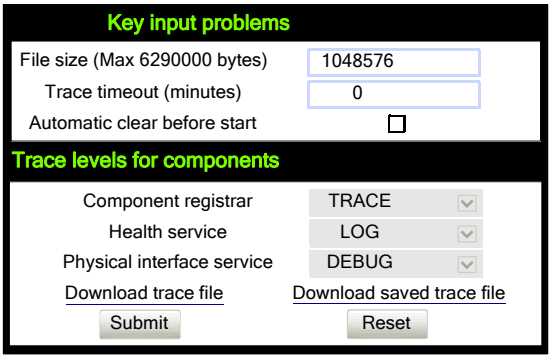

## DLS data errors



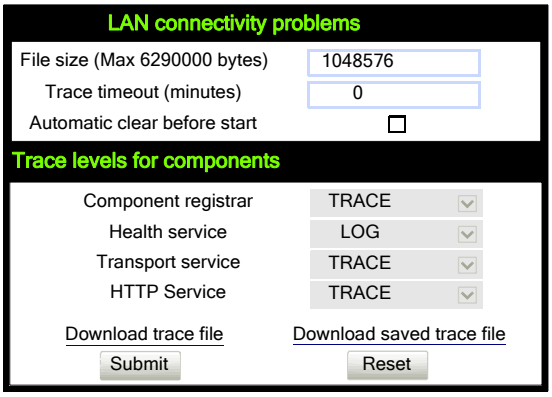
## Help application problems



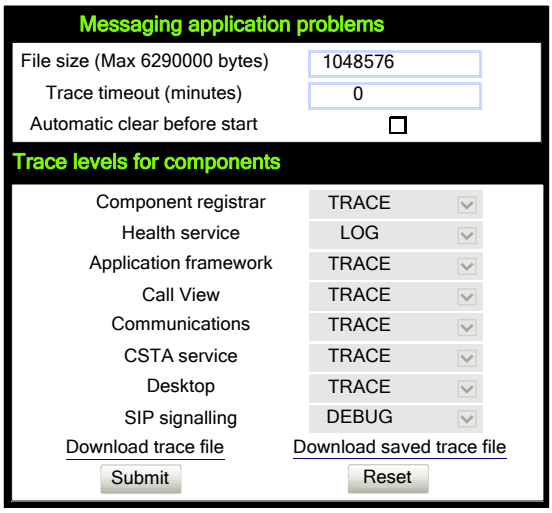

## Key input problems



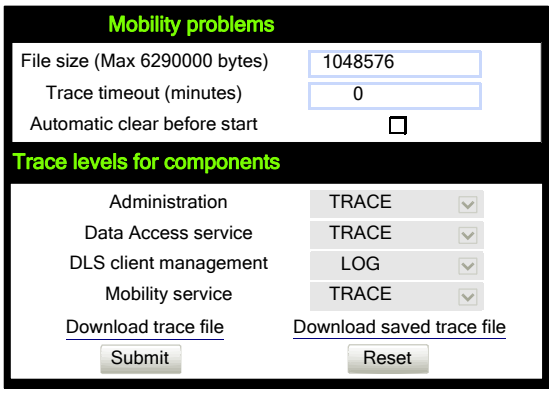

## LAN connectivity problems



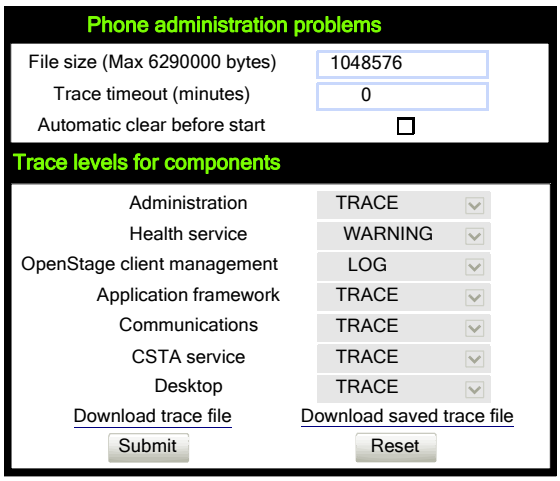
## Messaging application problems



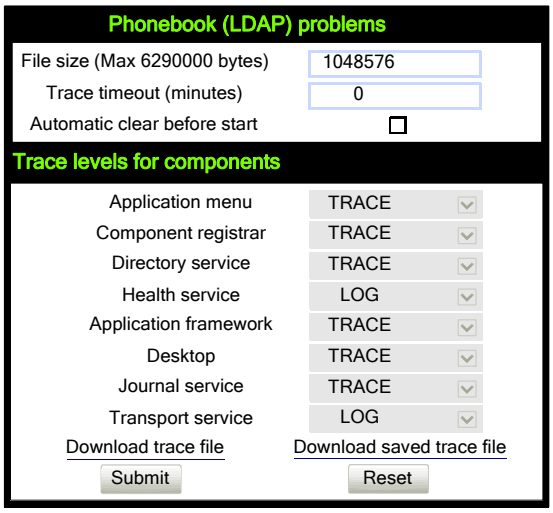

## Mobility problems



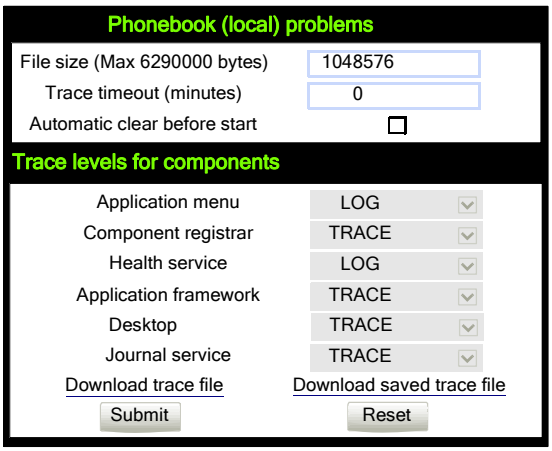
## Phone administration problems



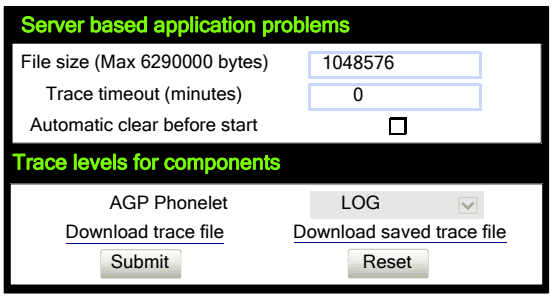

## Phonebook (LDAP) problems



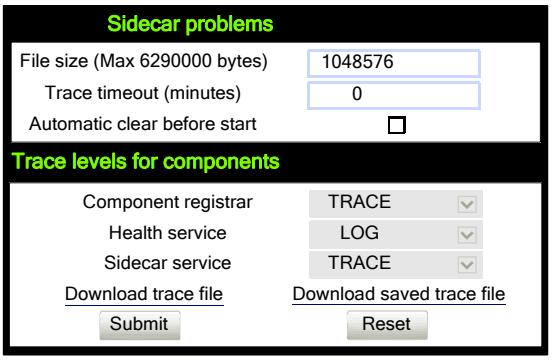
## Phonebook (local) problems



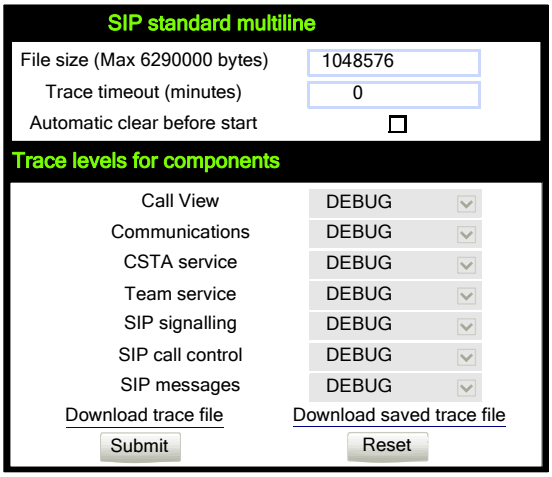

## Server based application problems



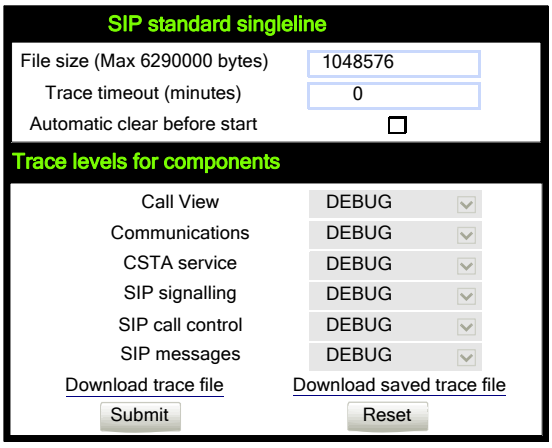

## Sidecar problems



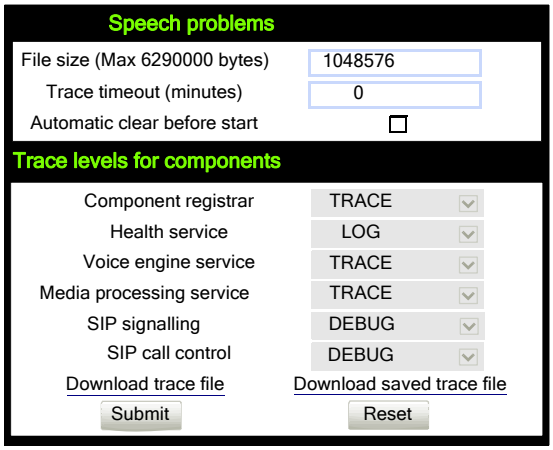
## SIP standard multiline



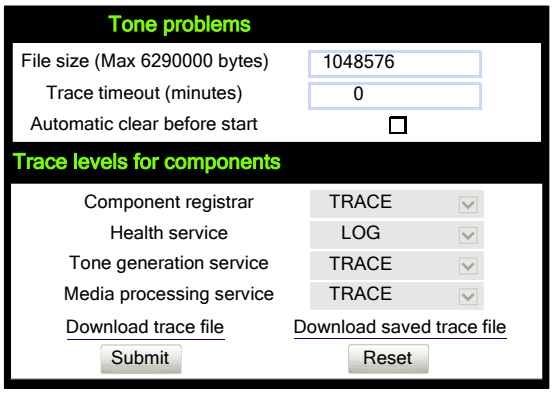

## SIP standard singleline



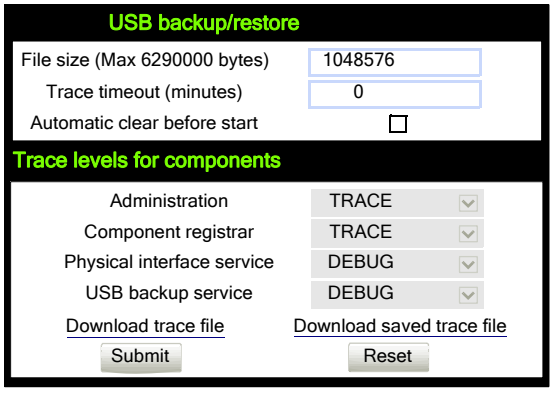
## Speech problems



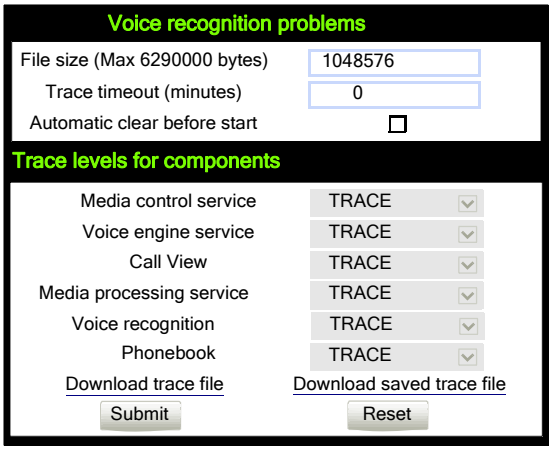

## Tone problems



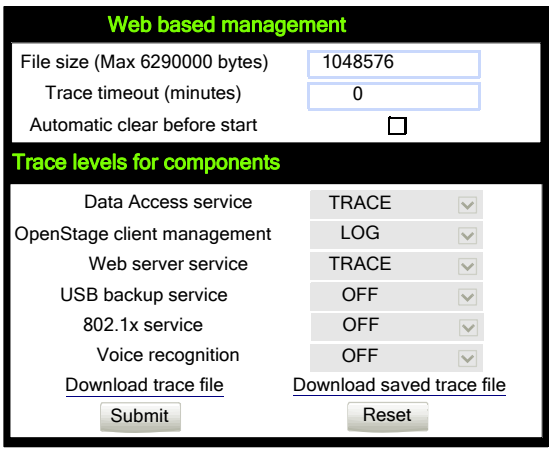

## USB backup/restore



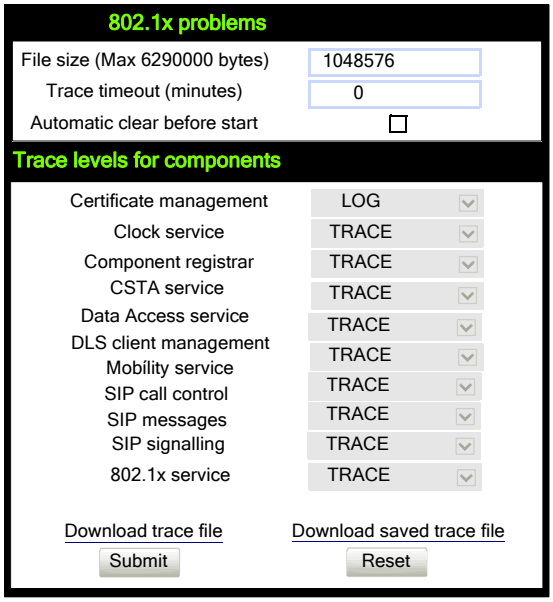
## Voice recognition problems



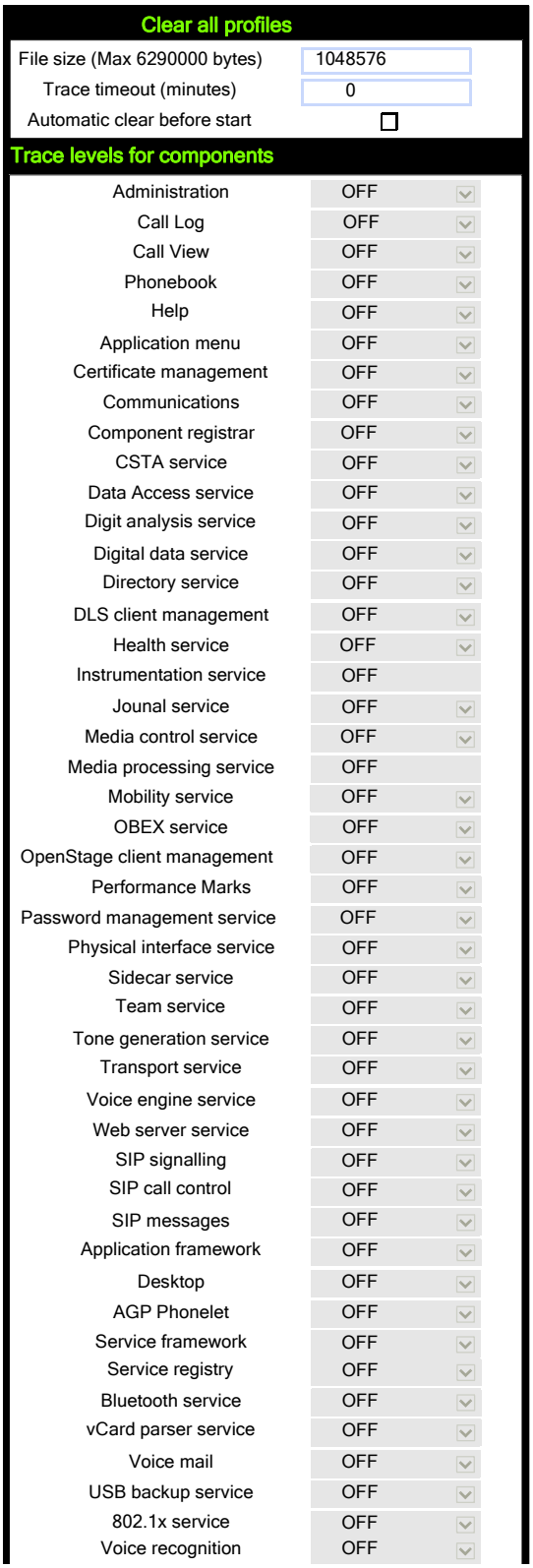

## Web based management



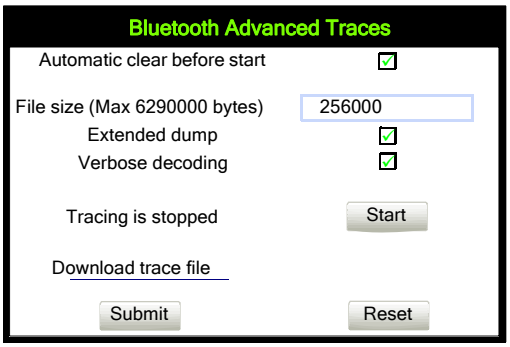
## 802.1x problems



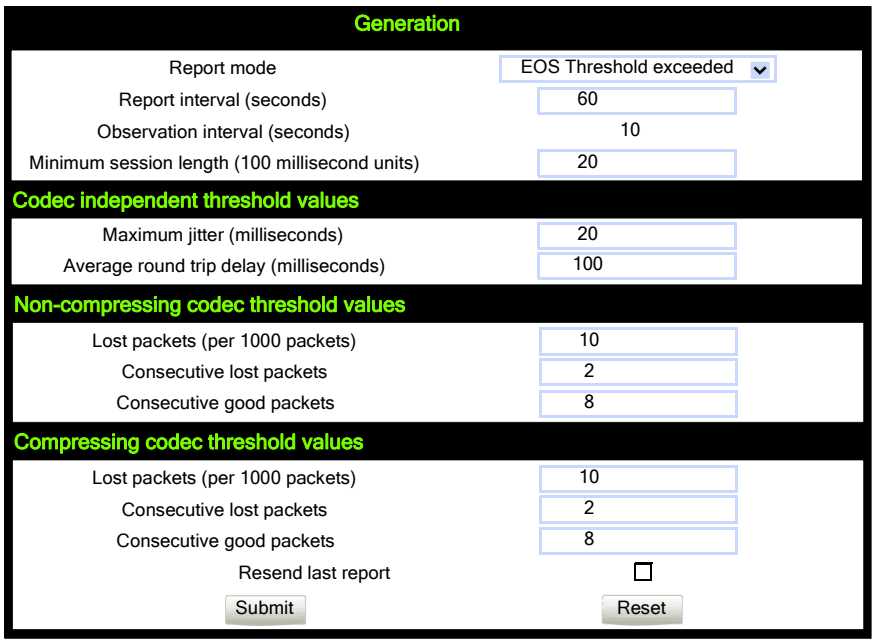
## Clear all profiles



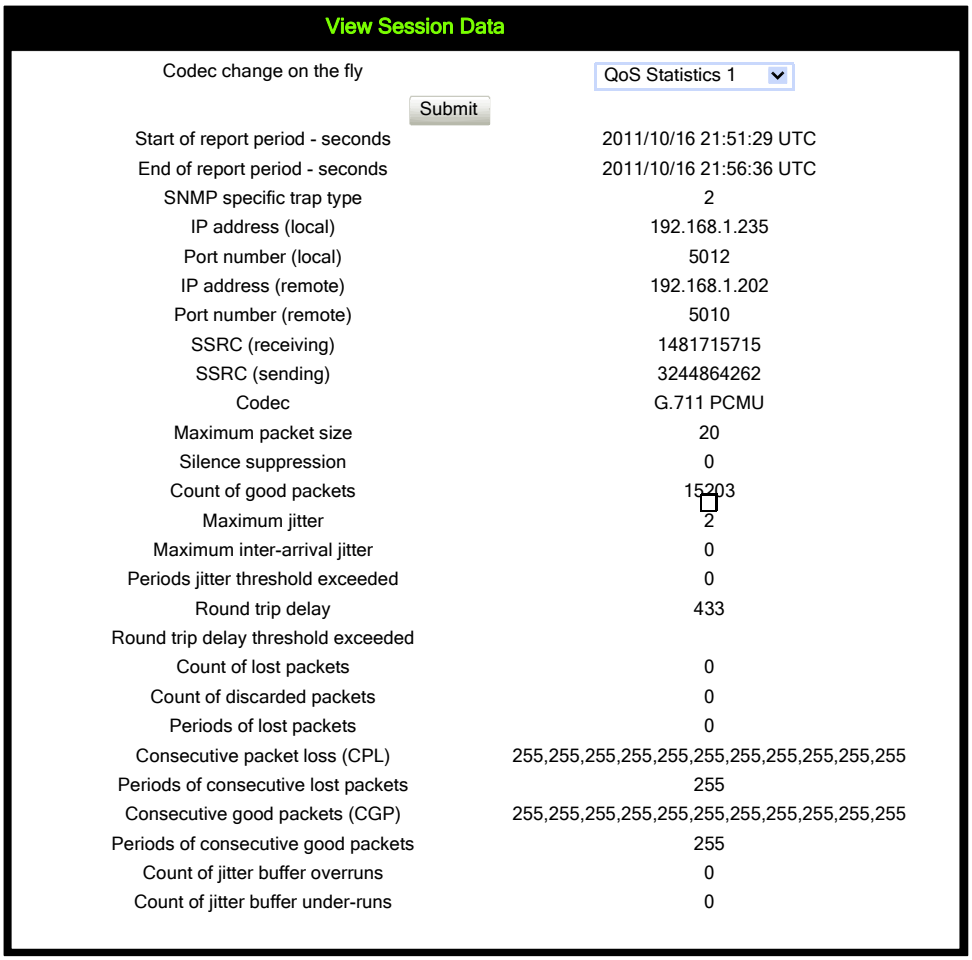
## Bluetooth Advanced Traces




## Generation



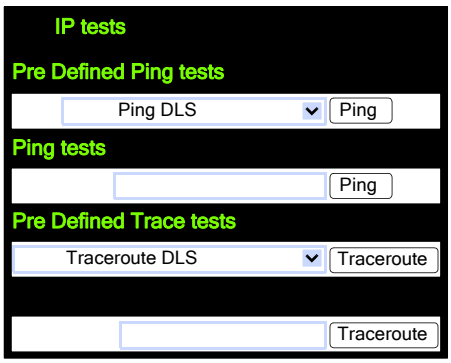
## View Session Data



View Session Data

| | |
|---|---|
| Codec change on the fly | QoS Statistics 1 |
| | Submit |
| Start of report period - seconds | 2011/10/16 21:51:29 UTC |
| End of report period - seconds | 2011/10/16 21:56:36 UTC |
| SNMP specific trap type | 2 |
| IP address (local) | 192.168.1.235 |
| Port number (local) | 5012 |
| IP address (remote) | 192.168.1.202 |
| Port number (remote) | 5010 |
| SSRC (receiving) | 1481715715 |
| SSRC (sending) | 3244864262 |
| Codec | G.711 PCMU |
| Maximum packet size | 20 |
| Silence suppression | 0 |
| Count of good packets | 15203 |
| Maximum jitter | 2 |
| Maximum inter-arrival jitter | 0 |
| Periods jitter threshold exceeded | 0 |
| Round trip delay | 433 |
| Round trip delay threshold exceeded | |
| Count of lost packets | 0 |
| Count of discarded packets | 0 |
| Periods of lost packets | 0 |
| Consecutive packet loss (CPL) | 255,255,255,255,255,255,255,255,255,255 |
| Periods of consecutive lost packets | 255 |
| Consecutive good packets (CGP) | 255,255,255,255,255,255,255,255,255,255 |
| Periods of consecutive good packets | 255 |
| Count of jitter buffer overruns | 0 |
| Count of jitter buffer under-runs | 0 |

## IP tests



IP tests

Pre Defined Ping tests

Ping DLS Ping

Ping tests

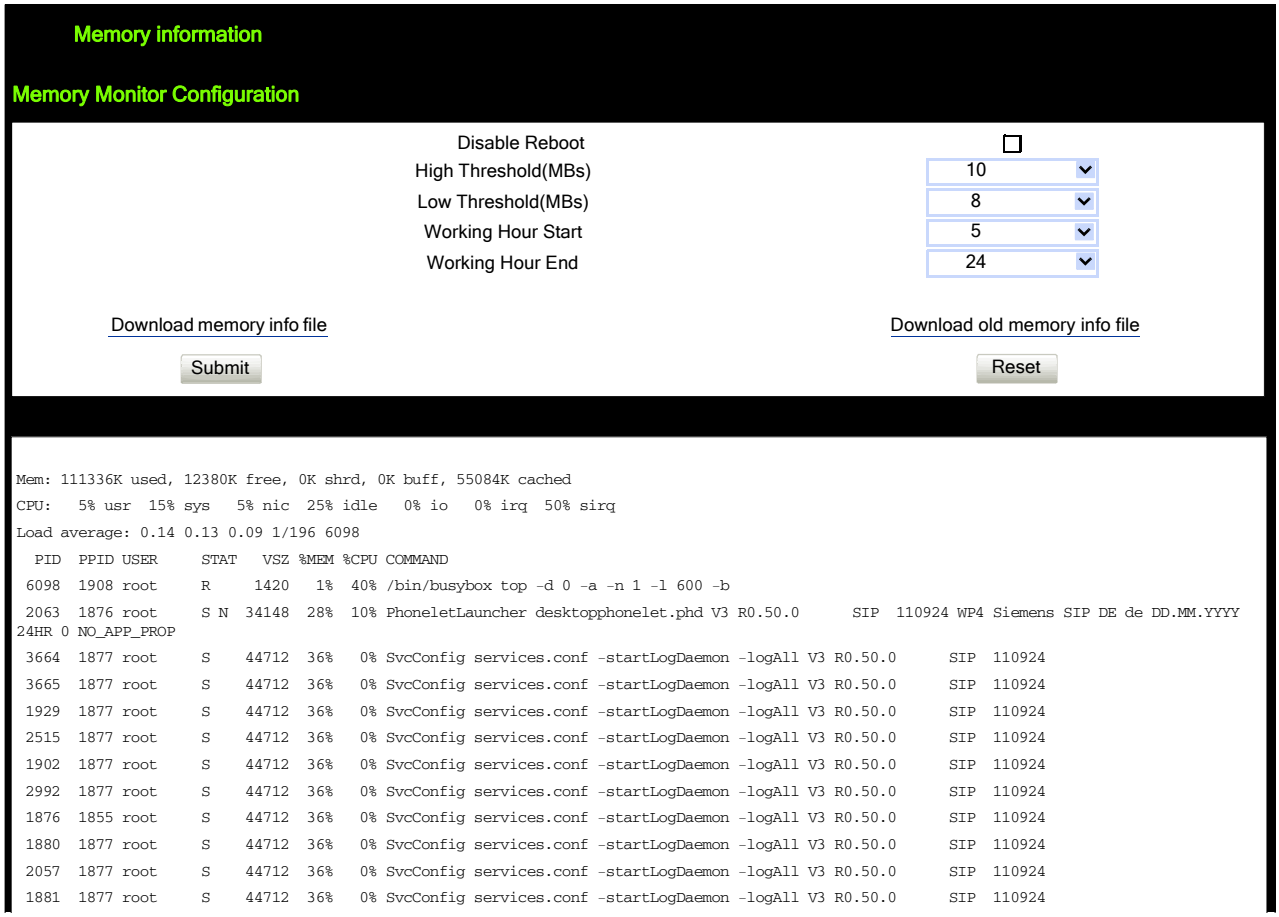
Ping

Pre Defined Trace tests

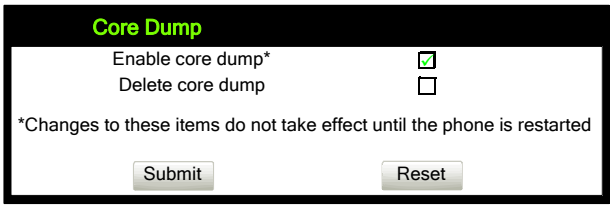
Traceroute DLS Traceroute

Traceroute

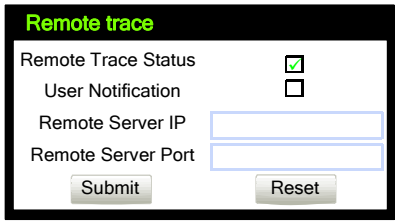
## Memory information


Memory information
Memory Monitor Configuration
Disable Reboot
High Threshold(MBs)
10
Low Threshold(MBs)
8
Working Hour Start
5
Working Hour End
24
Download memory info file
Download old memory info file
Submit
Reset
Mem: 111336K used, 12380K free, 0K shrd, 0K buff, 55084K cached
CPU: 5% usr 15% sys 5% nic 25% idle 0% io 0% irq 50% sirq
Load average: 0.14 0.13 0.09 1/196 6098
PID PPID USER STAT VSZ %MEM %CPU COMMAND
6098 1908 root R 1420 1% 40% /bin/busybox top -d 0 -a -n 1 -l 600 -b
2063 1876 root S N 34148 28% 10% PhoneletLauncher desktopphonelet.phd V3 R0.50.0 SIP 110924 WP4 Siemens SIP DE de DD.MM.YYYY 24HR 0 NO_APP_PROP
3664 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
3665 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1929 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2515 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1902 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2992 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1876 1855 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1880 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
2057 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924
1881 1877 root S 44712 36% 0% SvcConfig services.conf -startLogDaemon -logAll V3 R0.50.0 SIP 110924

## Core Dump

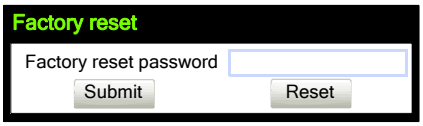



## Remote trace



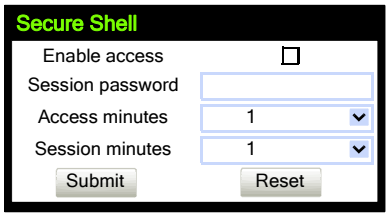
## Restart Phone

## Factory reset




## HPT interface

## Secure Shell




## Diagnostic call

## 4.1.2 Local Phone Menu

| **Menu** | **Further information ...** |
|---|---|
| --- Administration | |
| --- Applications (OpenStage 60/80 only) | |
| --- XML applications | |
| --- Add application: New phonebook application | -> Section 3.19.1.1 |
| --- Add application: New call log application | -> Section 3.19.1.1 |
| --- Add application: New messages application | -> Section 3.19.1.1 |
| --- Add Xpressions: Xpressions application | -> Section 3.19.1 |
| --- Add application: New help application | -> Section 3.19.1.1 |
| --- Network | |
| --- General IP configuration | |
| --- Protocol mode | -> Section 3.3.2 |
| --- Use LLDP-Med | -> Section 3.2.2 |
| --- Use DHCP | -> Section 3.3.3 |
| --- Use DHCPv6 | -> Section 3.3.3 |
| --- VLAN discovery | -> Section 3.2.2.2 |
| --- VLAN ID | -> Section 3.2.2.3 |
| --- DNS domain | -> Section 3.3.7.1 |
| --- Primary DNS | -> Section 3.3.7.2 |
| --- Secondary DNS | -> Section 3.3.7.2 |
| --- HTTP Proxy (OpenStage 60/80 only) | -> Section 3.19.1.2 |
| --- IPv4 configuration | |
| --- Use LLDP-Med | -> Section 3.2.2 |
| --- Use DHCP | -> Section 3.3.3 |
| --- DHCP reuse | -> Section 2.3.4 |
| --- IP address | -> Section 3.3.4 |
| --- Subnet mask | -> Section 3.3.4 |
| --- Route (default) | -> Section 3.3.5 |
| --- Route 1 IP | -> Section 3.3.7 |
| --- Route 1 gateway | -> Section 3.3.7 |
| --- Route 1 mask | -> Section 3.3.7 |
| --- Route 2 IP | -> Section 3.3.7 |
| --- Route 2 gateway | -> Section 3.3.7 |
| --- Route 2 mask | -> Section 3.3.7 |
| --- IPv6 configuration | |
| --- Use LLDP-Med | -> Section 3.2.2 |
| --- Use DHCPv6 | -> Section 3.3.3 |
| --- DHCPv6 reuse | -> Section 3.3.4.1 |
| --- Global address | -> Section 3.3.4.1 |
| --- Global prefix len | -> Section 3.3.4.1 |
| --- Global gateway | -> Section 3.3.4.1 |
| --- Link local address | -> Section 3.3.4.1 |
| --- Route 1 dest. | -> Section 3.3.4.1 |
| --- Route 1 prefix len. | -> Section 3.3.4.1 |
| --- Route 1 gateway | -> Section 3.3.4.1 |
| --- Route 2 dest. | -> Section 3.3.4.1 |
| --- Route 2 prefix len. | -> Section 3.3.4.1 |
| --- Route 2 gateway | -> Section 3.3.4.1 |

| Menu | Further information ... |
|---|---|
| --- Update Service (DLS) | |
| --- DLS address | -> Section 3.3.8 |
| --- DLS port | -> Section 3.3.8 |
| --- Contact gap | -> Section 3.3.8 |
| --- Mode | -> Section 3.3.8 |
| --- Security PIN | -> Section 3.3.8 |
| --- QoS | |
| --- Service | |
| --- Layer 2 | -> Section 3.3.1.1 |
| --- Layer 2 voice | -> Section 3.3.1.1 |
| --- Layer 2 signalling | -> Section 3.3.1.1 |
| --- Layer 2 default | -> Section 3.3.1.1 |
| --- Layer 3 | -> Section 3.3.1.2 |
| --- Layer 3 voice | -> Section 3.3.1.2 |
| --- Layer 3 signalling | -> Section 3.3.1.2 |
| --- MLPP (not used with OpenScape Voice) | |
| --- Reports | |
| --- Generation | |
| --- Mode | -> Section 3.26.12 |
| --- Report interval | -> Section 3.26.12 |
| --- Observe interval | -> Section 3.26.12 |
| --- Minimum session | -> Section 3.26.12 |
| --- Send now | -> Section 3.26.12.1 |
| --- Thresholds | |
| --- Max jitter | -> Section 3.26.12 |
| --- Round-trip delay | -> Section 3.26.12 |
| --- Non-compressing: | |
| --- ...Lost packets (K) | -> Section 3.26.12 |
| --- ...Lost consecutive | -> Section 3.26.12 |
| --- ...Good consecutive | -> Section 3.26.12 |
| --- Compressing: | |
| --- ...Lost packets (K) | -> Section 3.26.12 |
| --- ...Lost consecutive | -> Section 3.26.12 |
| --- ...Good consecutive | -> Section 3.26.12 |
| --- Port configuration | |
| --- SIP server | -> Section 3.5.6.2 |
| --- SIP registrar | -> Section 3.5.6.2 |
| --- SIP gateway | -> Section 3.5.6.2 |
| --- SIP local | -> Section 3.5.6.2 |
| --- Backup proxy | -> Section 3.5.10.5 |
| --- RTP base | -> Section 3.18.1 |
| --- LDAP Server port | -> Section 3.17.1 |
| --- LAN port type | -> Section 3.2.1 |
| --- PC port status | -> Section 3.2.1 |
| --- PC port type | -> Section 3.2.1 |
| --- PC port autoMDIX | -> Section 3.2.1 |
| --- HTTP proxy | -> Section 3.19.1.2 |
| --- LLDP-MED operation | |
| --- Extended Power | -> Section 3.26.6 |

| Menu | Further information ... |
|---|---|
| --- Network policy (voice) | -> Section 3.26.6 |
| --- LLDP-MED cap's | -> Section 3.26.6 |
| --- MAC_Phy config | -> Section 3.26.6 |
| --- System cap's | -> Section 3.26.6 |
| --- TTL - OK | -> Section 3.2.3 |
| --- System | |
| --- Identity | |
| --- Terminal number | -> Section 3.5.1.1 |
| --- Terminal name | -> Section 3.5.1.1 |
| --- Display identity | -> Section 3.5.1.2 |
| --- Enable ID | -> Section 3.5.1.2 |
| --- Web name | -> Section 3.3.7.3 |
| --- DDNS hostname | -> Section 3.3.7.3 |
| --- SIP Interface | |
| --- Outbound proxy | -> Section 3.5.8.1 |
| --- Default OBP domain | -> Section 3.5.8.1 |
| --- SIP transport | -> Section 3.5.8.2 |
| --- Call trans (ms) / Response timer (ms) | -> Section 3.5.10.2 |
| --- NonCall trans (ms) | -> Section 3.5.10.3 |
| --- Registration backoff | -> Section 3.5.10.4 |
| --- Connectivity timer (ms) | -> Section 3.5.10.1 |
| --- Keep alive format (not used with OS Voice) | |
| --- Media negotiation | -> Section 3.5.8.3 |
| --- Media IP mode | -> Section 3.5.8.3 |
| --- Registration | |
| --- SIP addresses | |
| --- SIP server | -> Section 3.5.6.1 |
| --- SIP registrar | -> Section 3.5.6.1 |
| --- SIP gateway | -> Section 3.5.6.1 |
| --- SIP session | |
| --- Session timer | -> Section 3.5.9 |
| --- Session duration (s) | -> Section 3.5.9 |
| --- Registration timer (s) | -> Section 3.5.7 |
| --- Server type | -> Section 3.5.7 |
| --- Realm | -> Section 3.5.7 |
| --- User ID | -> Section 3.5.7 |
| --- Password | -> Section 3.5.7 |
| --- MLPP base (not used with OpenScape Voice) | |
| --- MLPP Domain (not used with OpenScape Voice) | |
| --- Other Domain (not used with OpenScape Voice) | |
| --- SIP survivability | |
| --- Backup registration flag | -> Section 3.5.10.5 |
| --- Backup proxy address | -> Section 3.5.10.5 |
| --- Backup registration timer (s) | -> Section 3.5.10.5 |
| --- Backup transport | -> Section 3.5.10.5 |
| --- OBP flag | -> Section 3.5.10.5 |
| --- SNMP | |
| --- Queries allowed | -> Section 3.3.9 |
| --- Query password | -> Section 3.3.9 |

| Menu | Further information ... |
|---|---|
| --- Trap sending enabled | -> Section 3.3.9 |
| --- Trap destination | -> Section 3.3.9 |
| --- Trap destination port | -> Section 3.3.9 |
| --- Trap community | -> Section 3.3.9 |
| --- Diagnostic sending enabled | -> Section 3.3.9 |
| --- Diagnostic destination | -> Section 3.3.9 |
| --- Diagnostic destination port | -> Section 3.3.9 |
| --- Diagnostic community | -> Section 3.3.9 |
| --- QoS traps to QCU | -> Section 3.3.9 |
| --- QCU address | -> Section 3.3.9 |
| --- QCU port | -> Section 3.3.9 |
| --- QCU community | -> Section 3.3.9 |
| --- QoS to generic destination | -> Section 3.3.9 |
| --- Features | |
| --- Configuration | |
| --- General | |
| --- Emergency number | -> Section 3.5.2 |
| --- Voicemail number | -> Section 3.5.2 |
| --- MWI LED | -> Section 3.28 |
| --- Missed Call LED | -> Section 3.29 |
| --- Allow refuse | -> Section 3.7.1 |
| --- Hot / warm phone | -> Section 3.7.2 |
| --- Hot / warm destination | -> Section 3.7.2 |
| --- Initial digit timer | -> Section 3.7.3 |
| --- Allow uaCSTA | -> Section 3.7.11 |
| --- Server features | -> Section 3.7.10 |
| --- Transfer on hangup | -> Section 3.7.5.2 |
| --- Not used timeout | -> Section 3.7.12 |
| --- DSS Pickup timer | -> Section 3.11.5.1 |
| --- Bridging enabled | -> Section 3.11.2 |
| --- Dial plan | -> Section 3.13.4 |
| --- FPK prog. timer | -> Section 3.8 |
| --- Audio | |
| --- Pickup tone allowed | -> Section 3.7.4.2 |
| --- Pickup as ringer | -> Section 3.7.4.2 |
| --- Pickup visual alert | -> Section 3.7.4.2 |
| --- BLF alerting | -> Section 3.7.4.2 |
| --- MLPP ringer (not used with OpenScape Voice) | |
| --- Callback ringer | -> Section 3.7.6.1 |
| --- Lower IL ringer | -> Section 3.30 |
| --- Keyset Lines (OpenStage 15/40/60/80) | |
| --- Details For Keyset Line <n> | |
| --- Address | -> Section 3.11.1 |
| --- Ring on/off | -> Section 3.11.1 |
| --- Selection order | -> Section 3.11.1 |
| --- Hot/warm action | -> Section 3.11.1 |
| --- Call recording | |
| --- Recorder number | -> Section 3.7.13 |
| --- Recording mode | -> Section 3.7.13 |
| --- Audible notification | -> Section 3.7.13 |

| Menu | Further information ... |
|---|---|
| Keyset operation (OpenStage 15/40/60/80 only) | |
| Rollover ring | -> Section 3.11.2 |
| LED on registration | -> Section 3.11.2 |
| Originating line preference | -> Section 3.11.2 |
| Terminating line preference | -> Section 3.11.2 |
| Line action mode | -> Section 3.11.2 |
| Show focus | -> Section 3.11.2 |
| Reservation timer | -> Section 3.11.2 |
| Forwarding indicated / Forwarding shown | -> Section 3.11.2 |
| Preselect mode | -> Section 3.11.2 |
| Preselect timer | -> Section 3.11.2 |
| Preview mode | -> Section 3.11.3 |
| Preview timer | -> Section 3.11.3 |
| Bridging priority | -> Section 3.11.3 |
| DSS operation (OpenStage 15/40/60/80 only) | |
| Deflect to DSS | -> Section 3.11.5.1 |
| Refuse DSS pickup | -> Section 3.11.5.1 |
| Forwarding shown | -> Section 3.11.5.1 |
| Addressing | |
| MWI server URI | -> Section 3.7.7 |
| Conference | -> Section 3.7.9 |
| Group pickup URI | -> Section 3.7.4 |
| Callback FAC | -> Section 3.7.6 |
| Callback: busy (upto V2R2) | -> Section 3.7.6 |
| Callback: no reply (upto V2R2) | -> Section 3.7.6 |
| Callback: cancel all | -> Section 3.7.6 |
| BLF pickup code | -> Section 3.7.4 |
| Call completion | |
| Functional CCSS | -> Section 3.7.6.1 |
| Callback ringer | -> Section 3.7.6.1 |
| Allow after call (s) | -> Section 3.7.6.1 |
| Max. callbacks | -> Section 3.7.6.1 |
| Feature Access | |
| Call control | |
| Blind transfer | -> Section 3.6 |
| 3rd call leg | -> Section 3.6 |
| Call establish | |
| Callback | -> Section 3.6 |
| Call pickup | -> Section 3.6 |
| Group pickup | -> Section 3.6 |
| Call deflection | -> Section 3.6 |
| Call forwarding | -> Section 3.6 |
| Do not disturb | -> Section 3.6 |
| Refuse call | -> Section 3.6 |
| Repertory dial key | -> Section 3.6 |
| Ext/int forwarding | -> Section 3.6 |
| Call associated | |
| Phone book lookups | -> Section 3.6 |
| DSS feature | -> Section 3.6 |
| BLF feature | -> Section 3.6 |
| Line overview | -> Section 3.6 |

| Menu | Further information ... |
|---|---|
| Video calls | -> Section 3.6 |
| CTI | |
| CTI control | -> Section 3.6 |
| Services | |
| Bluetooth | -> Section 3.6 |
| Web based mang. | -> Section 3.6 |
| USB device access | -> Section 3.6 |
| Backup to USB | -> Section 3.6 |
| Feature togggle | -> Section 3.6 |
| Phone lock | -> Section 3.6 |
| Security | |
| System | |
| Server certificate | -> Section 3.4 |
| Use secure calls | -> Section 3.4 |
| SRTP type | -> Section 3.4 |
| Use SRTCP | -> Section 3.4 |
| SDES config | |
| SDES status | -> Section 3.4.1.3 |
| SDP negotiation | -> Section 3.4.1.3 |
| SHA1-80 crypto | -> Section 3.4.1.3 |
| SHA1-32 crypto | -> Section 3.4.1.3 |
| Access control | |
| CCE access | -> Section 3.4.2 |
| Factory reset claw | -> Section 3.4.2 |
| Serial port | -> Section 3.4.2 |
| Logging | |
| Max. lines | -> Section 3.4.3 |
| Archive to DLS | -> Section 3.4.3 |
| Last archived | -> Section 3.4.3 |
| Archive when at | -> Section 3.4.3 |
| Faults | |
| Security log entry | -> Section 3.4.4 |
| OCSR failure | -> Section 3.4.4 |
| Admin access | -> Section 3.4.4 |
| User access | -> Section 3.4.4 |
| File Transfer | |
| Defaults | -> Section 3.16.2 |
| Download method | -> Section 3.16.2 |
| Server | -> Section 3.16.2 |
| Port | -> Section 3.16.2 |
| Account | -> Section 3.16.2 |
| Username | -> Section 3.16.2 |
| Password | -> Section 3.16.2 |
| FTP path | -> Section 3.16.2 |
| HTTPS base URL | -> Section 3.16.2 |
| Phone app | -> Section 3.16.3 |
| Use default | -> Section 3.16.3.1 |
| Download method | -> Section 3.16.3.1 |
| Server | -> Section 3.16.3.1 |

| Menu | Further information ... |
|---|---|
| --- Port | -> Section 3.16.3.1 |
| --- Account | -> Section 3.16.3.1 |
| --- Username | -> Section 3.16.3.1 |
| --- Password | -> Section 3.16.3.1 |
| --- FTP path | -> Section 3.16.3.1 |
| --- HTTPS base URL | -> Section 3.16.3.1 |
| --- Filename | -> Section 3.16.3.1 |
| --- Hold music | |
| --- Use default | -> Section 3.16.4.1 |
| --- Download method | -> Section 3.16.4.1 |
| --- Server | -> Section 3.16.4.1 |
| --- Port | -> Section 3.16.4.1 |
| --- Account | -> Section 3.16.4.1 |
| --- Username | -> Section 3.16.4.1 |
| --- Password | -> Section 3.16.4.1 |
| --- FTP path | -> Section 3.16.4.1 |
| --- HTTPS base URL | -> Section 3.16.4.1 |
| --- Filename | -> Section 3.16.4.1 |
| --- Ringer | |
| --- Use default | -> Section 3.16.6.1 |
| --- Download method | -> Section 3.16.6.1 |
| --- Server | -> Section 3.16.6.1 |
| --- Port | -> Section 3.16.6.1 |
| --- Account | -> Section 3.16.6.1 |
| --- Username | -> Section 3.16.6.1 |
| --- Password | -> Section 3.16.6.1 |
| --- FTP path | -> Section 3.16.6.1 |
| --- HTTPS base URL | -> Section 3.16.6.1 |
| --- Filename | -> Section 3.16.6.1 |
| --- Picture clip (OpenStage 60/80 only) | |
| --- Use default | -> Section 3.16.5.1 |
| --- Download method | -> Section 3.16.5.1 |
| --- Server | -> Section 3.16.5.1 |
| --- Port | -> Section 3.16.5.1 |
| --- Account | -> Section 3.16.5.1 |
| --- Username | -> Section 3.16.5.1 |
| --- Password | -> Section 3.16.5.1 |
| --- FTP path | -> Section 3.16.5.1 |
| --- HTTPS base URL | -> Section 3.16.5.1 |
| --- Filename | -> Section 3.16.5.1 |
| --- LDAP | |
| --- Use default | -> Section 3.16.6.1 |
| --- Download method | -> Section 3.16.6.1 |
| --- Server | -> Section 3.16.6.1 |
| --- Port | -> Section 3.16.6.1 |
| --- Account | -> Section 3.16.6.1 |
| --- Username | -> Section 3.16.6.1 |
| --- Password | -> Section 3.16.6.1 |
| --- FTP path | -> Section 3.16.6.1 |
| --- HTTPS base URL | -> Section 3.16.6.1 |
| --- Filename | -> Section 3.16.6.1 |

| Menu | Further information ... |
|---|---|
| --- Logo (OpenStage 40/60/80 only) | |
| --- Use default | -> Section 3.16.7.1 |
| --- Download method | -> Section 3.16.7.1 |
| --- Server | -> Section 3.16.7.1 |
| --- Port | -> Section 3.16.7.1 |
| --- Account | -> Section 3.16.7.1 |
| --- Username | -> Section 3.16.7.1 |
| --- Password | -> Section 3.16.7.1 |
| --- FTP path | -> Section 3.16.7.1 |
| --- HTTPS base URL | -> Section 3.16.7.1 |
| --- Filename | -> Section 3.16.7.1 |
| --- Screensaver (OpenStage 60/80 only) | |
| --- Use default | -> Section 3.16.8.1 |
| --- Download method | -> Section 3.16.8.1 |
| --- Server | -> Section 3.16.8.1 |
| --- Port | -> Section 3.16.8.1 |
| --- Account | -> Section 3.16.8.1 |
| --- Username | -> Section 3.16.8.1 |
| --- Password | -> Section 3.16.8.1 |
| --- FTP path | -> Section 3.16.8.1 |
| --- HTTPS base URL | -> Section 3.16.8.1 |
| --- Filename | -> Section 3.16.8.1 |
| --- HPT dongle | |
| --- Use default | -> Section 3.16.10 |
| --- Download method | -> Section 3.16.10 |
| --- Server | -> Section 3.16.10 |
| --- Port | -> Section 3.16.10 |
| --- Account | -> Section 3.16.10 |
| --- Username | -> Section 3.16.10 |
| --- Password | -> Section 3.16.10 |
| --- FTP path | -> Section 3.16.10 |
| --- HTTPS base URL | -> Section 3.16.10 |
| --- Filename | -> Section 3.16.10 |
| --- Local Functions | |
| --- Directory Settings / LDAP | |
| --- (LDAP) server address | -> Section 3.17.1 |
| --- (LDAP) server port | -> Section 3.17.1 |
| --- (LDAP) Authenticate / Authentication | -> Section 3.17.1 |
| --- (LDAP) User name | -> Section 3.17.1 |
| --- (LDAP) Password | -> Section 3.17.1 |
| --- Timeout (sec) for / Search Trigger (s) | -> Section 3.17.1 |
| --- Locality | |
| --- Canonical settings | |
| --- Local country code | -> Section 3.13.1 |
| --- National prefix digit | -> Section 3.13.1 |
| --- Local national code | -> Section 3.13.1 |
| --- Minimum local number length | -> Section 3.13.1 |
| --- Local enterprise node | -> Section 3.13.1 |
| --- PSTN access code | -> Section 3.13.1 |
| --- International access code | -> Section 3.13.1 |

| Menu | Further information ... |
|---|---|
| --- Operator code | -> Section 3.13.1 |
| --- Emergency number | -> Section 3.13.1 |
| --- Initial digits | -> Section 3.13.1 |
| --- Canonical lookup | |
| --- Local code 1 | -> Section 3.13.2 |
| --- International 1 | -> Section 3.13.2 |
| --- Local code 2 | -> Section 3.13.2 |
| --- International 2 | -> Section 3.13.2 |
| --- Local code 3 | -> Section 3.13.2 |
| --- International 3 | -> Section 3.13.2 |
| --- Local code 4 | -> Section 3.13.2 |
| --- International 4 | -> Section 3.13.2 |
| --- Local code 5 | -> Section 3.13.2 |
| --- International 5 | -> Section 3.13.2 |
| --- Canonical dial | |
| --- Internal numbers | -> Section 3.13.1 |
| --- External numbers | -> Section 3.13.1 |
| --- External access | -> Section 3.13.1 |
| --- International gateway / International access | -> Section 3.13.1 |
| --- Energy saving (OpenStage 40/60/80 only) | |
| --- Backlight timeout | -> Section 3.5.3 |
| --- Messages settings | |
| --- New items | -> Section 3.7.8 |
| --- Alternative label | -> Section 3.7.8 |
| --- New urgent items | -> Section 3.7.8 |
| --- Alternative label | -> Section 3.7.8 |
| --- Old items | -> Section 3.7.8 |
| --- Alternative label | -> Section 3.7.8 |
| --- Old urgent items | -> Section 3.7.8 |
| --- Alternative label | -> Section 3.7.8 |
| --- Call logging | |
| --- FAC prefixes | -> Section 3.5.4 |
| --- Date and Time | |
| --- Time source | |
| --- SNTP IP address | -> Section 3.5.5.1 |
| --- Timezone offset | -> Section 3.5.5.1 |
| --- Daylight saving | -> Section 3.5.5.1 |
| --- Daylight saving | -> Section 3.5.5.1 |
| --- Difference (mins) | -> Section 3.5.5.1 |
| --- Auto DST | -> Section 3.5.5.1 |
| --- DST zone | -> Section 3.5.5.1 |
| --- Speech | |
| --- Codec preferences | |
| --- Silence suppression | -> Section 3.18.2 |
| --- Packet size | -> Section 3.18.2 |
| --- G.711 | -> Section 3.18.2 |
| --- G.729 | -> Section 3.18.2 |
| --- G.722 | -> Section 3.18.2 |
| --- Allow “HD” icon | -> Section 3.18.2 |

| Menu | Further information ... |
|---|---|
| └── Audio settings | |
| ├── Disable microphone | -> Section 3.18.3 |
| ├── Disable loudspeech | -> Section 3.18.3 |
| └── DTMF playback | -> Section 3.18.3 |
| ├── General information | |
| ├── MAC address | -> Section 3.26.1 |
| ├── Software version | -> Section 3.26.1 |
| ├── Last restart | -> Section 3.26.1 |
| ├── Dial plan ID | -> Section 3.13.4 |
| └── Dial plan status | -> Section 3.13.4 |
| ├── Licence information | -> Section 3.25 |
| ├── Password (up to V2R1) | |
| ├── Admin | -> Section 3.20 |
| ├── Confirm admin | -> Section 3.20 |
| ├── User | -> Section 3.20 |
| └── Confirm user | -> Section 3.20 |
| ├── Security & policies | |
| ├── Password | |
| ├── Generic policy | |
| ├── Expires after (days) | -> Section 3.4.5.1 |
| ├── Warn before (days) | -> Section 3.4.5.1 |
| ├── Force changed | -> Section 3.4.5.1 |
| ├── Tries allowed | -> Section 3.4.5.1 |
| ├── No change for (hours) | -> Section 3.4.5.1 |
| ├── Suspended for (mins) | -> Section 3.4.5.1 |
| └── History valid for (days) | -> Section 3.4.5.1 |
| ├── Admin policy | |
| ├── Expiry date | -> Section 3.4.5.2 |
| ├── Minimum length | -> Section 3.4.5.2 |
| ├── Password history | -> Section 3.4.5.2 |
| └── Current status | -> Section 3.4.5.2 |
| ├── User policy | |
| ├── Expiry date | -> Section 3.4.5.3 |
| ├── Minimum length | -> Section 3.4.5.3 |
| ├── Password history | -> Section 3.4.5.3 |
| └── Current status | -> Section 3.4.5.3 |
| ├── Character set | |
| ├── Ucase chars reqd. | -> Section 3.4.5.4 |
| ├── Lcase chars reqd. | -> Section 3.4.5.4 |
| ├── Digits required | -> Section 3.4.5.4 |
| ├── Special chars reqd. | -> Section 3.4.5.4 |
| ├── Bar repeat length | -> Section 3.4.5.4 |
| └── Min char difference | -> Section 3.4.5.4 |
| ├── Change admin password | |
| ├── Current password | -> Section 3.4.5.5 |
| ├── New password | -> Section 3.4.5.5 |
| └── Confirm password | -> Section 3.4.5.5 |

| Menu | Further information ... |
|---|---|
| Change User password | -> Section 3.4.5.5 |
| Admin password | -> Section 3.4.5.5 |
| New password | -> Section 3.4.5.5 |
| Confirm password | -> Section 3.4.5.5 |
| Certificates | |
| Generic | |
| OCSP check | -> Section 3.4.6.1 |
| OCSR 1 address | -> Section 3.4.6.1 |
| OCSR 2 address | -> Section 3.4.6.1 |
| Authentication policy | |
| Secure file transfer | -> Section 3.4.6.2 |
| Secure send URL | -> Section 3.4.6.2 |
| Secure SIP server | -> Section 3.4.6.2 |
| Secure 802.1x | -> Section 3.4.6.2 |
| Secure XML appl. | -> Section 3.4.6.2 |
| Ringer setting | |
| Distinctive | |
| <1 .... 15> | |
| Name | -> Section 3.14 |
| Ringer sound | -> Section 3.14 |
| Pattern melody | -> Section 3.14 |
| Pattern sequence | -> Section 3.14 |
| Duration | -> Section 3.14 |
| Audible | -> Section 3.14 |
| Map to Specials | -> Section 3.14.2 |
| Internal | |
| External | |
| Recall | |
| Emergency | |
| Special1 | |
| Special2 | |
| Special3 | |
| Mobility | |
| Unauthorized logoff trap | -> Section 3.15 |
| Logoff trap delay | -> Section 3.15 |
| Timer med priority | -> Section 3.15 |
| Mobility feature | -> Section 3.15 |
| Managed profile | |
| Error count local | |
| Diagnostic information | |
| View | -> Section 3.26.2 |
| Configure | -> Section 3.26.3 |
| Allow user | |
| Maintenance | |
| Factory reset | -> Section 3.23 |
| Disable HPT | -> Section 3.26.15 |
| Remote trace | |

| Menu | Further information ... |
|---|---|
| ├── Trace status | -> Section 3.26.14 |
| ├── User notification | -> Section 3.26.14 |
| ├── Remote server | -> Section 3.26.14 |
| └── Remote port | -> Section 3.26.14 |
| ├── Memory monitor | |
| ├── Disable reboot | -> Section 3.26.8 |
| ├── High threshold | -> Section 3.26.8 |
| ├── Low threshold | -> Section 3.26.8 |
| ├── Working Hour start | -> Section 3.26.8 |
| └── Working Hour end | -> Section 3.26.8 |
| └── Diagnostic call | |
| └── Prefix code | -> Section 3.26.4 |

## 4.2 Default Port List

The following table contains all default ports, resp. port ranges, and protocols used by the services running on OpenStage SIP phones.

| Service | Server Default Port | Client Default Port | Protocol Stack |
|---|---|---|---|
| Payload transport (VoIP) | 5010 - 5059 | 5010 - 5059 | RTP - RTCP |
| Payload transport (VoIP) | 5010 - 5059 | 5010 - 5059 | SRTP - SRTCP |
| SIP subscriber - TCP is used | 5060 | 32786 - 61000 | SIP / TCP |
| SIP subscriber - TLS is used | 5061 | 32786 - 61000 | SIP / TLS |
| SIP subscriber - UDP is used | 5060 | 5060 | SIP / UDP |
| XML applications in phone, connecting to an application server | --- | 32786 - 61000 | HTTP / TCP<br>HTTPS / TCP-TLS |
| XML Push service | 8085 | --- | HTTP / TCP |
| XML Push service | 443 | --- | HTTPS / TCP-TLS |
| Directory access via LDAP | --- | 32786 - 61000 | TCP |
| Directory access via LDAP | --- | 32786 - 61000 | TCP- SSL/TLS |
| DHCP Client | --- | 68 | DHCP / UDP |
| DNS Client | --- | 1024 - 65535 | DNS / TCP_UDP |
| DLS contact me service - workpoint side | 8085 | --- | HTTP / TCP |
| Default communication with the DLS workpoint interface | --- | 18443 | HTTPS / TCP - SSL / TLS |
| Secure communication with the DLS workpoint interface | --- | 18444 | HTTPS / TCP - SSL / TLS |
| Connection to the control port of FTP server | 21 | 32786 - 61000 | FTP / TCP |
| FTP client; uses the FTP server in active mode | 32786 - 61000 | 20 | FTP / TCP |
| HTTPS file download server | 443 | 32786 - 61000 | HTTPS / TCP - SSL/TLS |
| Client application which sends QDC data to the QCU | --- | 32786 - 61000 | SNMP / UDP |
| Part of SNMP-Agent - sending Traps | --- | 32786 - 61000 | SNMP / UDP |
| Part of SNMP-Agent - receive Set/ Get commands | 161 | --- | SNMP / UDP |

| Service | Server Default Port | Client Default Port | Protocol Stack |
|---|---|---|---|
| SNTP client - queries time information in unicast operation | --- | 123 | SNTP / UDP |
| SNTP client - receives time information in broadcast operation | 123 | --- | SNTP / UDP |
| Web server for WBM access | 8085 | --- | HTTP / TCP |
| Secure Web Server for WBM access | 443 | --- | HTTPS / TCP - SSL / TLS |
| OpenStage Phone Manager | 65532 | --- | TCP - SSL/TLS |
| Remote Trace | --- | 514 | UDP |
| HPT- debug IF (Available only if a dongle file is present on phone.) | 65532 | --- | TCP - SSL/TLS |
| SSH (Secure Shell Remote Login) | 22 | --- | TCP |
| Syslog Client (sends Traces to Syslog Server) | --- | 32786 - 61000 | UDP |
| Video H.263 | 5050-5059 | 5050-5059 | RTP - RTCP |
| Secure Video H.263 | 5050-5059 | 5050-5059 | SRTP - SRTCP |

## 4.3 Troubleshooting: Error Codes

For a set of error cases, specific error codes are defined. These error codes are shown in brackets on the display, following a general error note. Example: „No Telephony possible (LP1)“.

| Problem | Description | Error code |
|---|---|---|
| Network Problem | No network connection | LI1 |
| Not Initialised | Waiting for data | I1 |
| Unable to use LAN | 802.1x error | LX1 |
| Unable to use LAN | Physical connection missing | LP1 |
| Unable to Register | Server timeout | RT2 |
| Unable to Register | Server failed | RF2 |
| Unable to Register | Authentication failed | RA2 |
| Unable to Register | No number configured | RN2 |
| Unable to Register | No server configured | RS2 |
| Unable to Register | No registrar configured | RG2 |
| Unable to Register | No DNS domain configured | RD2 |
| Unable to Register | Rejected by server | RR2 |
| Unable to Register | No phone IP address set | RI2 |
| Survivability | Backup route active | B8 |
| Survivability | Backup not configured | RS8 |
| Survivability | Backup timeout | RT8 |
| Survivability | Backup authentication failed | RA8 |
| Cloud-Deployment abandoned by user | Cloud-Deployment abandoned by user Occurs when the pin prompt is dismissed | AU |
| Cloud-Deployment: unable to get the address for the SEN Redirect server | Cloud-Deployment: unable to get the address for the SEN Redirect server. DNS lookup failed | RS |
| Unable to establish contact with SEN Redirect server - no reply | Cloud-Deployment: unable to establish contact with SEN Redirect server - no reply | RN |

Tabelle 4-1 Troubleshooting Error Codes

| Problem | Description | Error code |
|---|---|---|
| Unable to establish contact with SEN Redirect server - refused | Cloud-Deployment: unable to establish contact with SEN Redirect server - refused | RR |
| Unable to establish contact with SEN Redirect server - unauthorised | Cloud-Deployment: unable to establish contact with SEN Redirect server - unauthorised | RU |
| Unable to establish contact with SEN Redirect server - no or invalid OCSP response | Cloud-Deployment: unable to establish contact with SEN Redirect server - no or invalid OCSP response | RO |
| Unable to establish contact with SEN Redirect server - certificate revoked | Cloud-Deployment: unable to establish contact with SEN Redirect server - certificate revoked | RV |
| Unable to get the address for the Deployment server | Cloud-Deployment: unable to get the address for the Deployment server. DNS lookup failed | DS |
| Unable to establish contact with Deployment server | Cloud-Deployment: unable to establish contact with Deployment server - no reply | DN |
| Unable to establish contact with Deployment server - refused | Cloud-Deployment: unable to establish contact with Deployment server - refused | DR |

Tabelle 4-1 Troubleshooting Error Codes

A special “fast-busy” tone (also called congestion tone) is played if a temporary network problem causes a user-initiated call action to fail. Typical call actions: making an outgoing call; picking up a call from Manual Hold; or Group pickup. Phone users include keyset users and mobile users logged on to the phone. The special tone is triggered if one of the following SIP response codes is received from the server: 606, 408, or 503.

http://wiki.unify.com/wiki/OpenStage_SIP_FAQ#Error_codes

# 5 Examples and HowTos

## 5.1 Canonical Dialing

### 5.1.1 Canonical Dialing Settings

The following example shows settings suitable for the conversion of given dial strings to canonical format. The example phone is located in Nottingham, UK.

| Parameter | Example value | Explanation |
|---|---|---|
| Local country code | 44 | International country code for the UK. |
| National prefix digit | 0 | Used in front of national codes when dialled without international prefix. |
| Local national code | 115 | Area code within the UK (here: Nottingham). |
| Minimum local number length | 7 | Minimum number of digits in a local PSTN number (e. g. 3335333 = 7 digits). |
| Local enterprise node | 780 | Prefix to access Nottingham numbers from within the Siemens network. |
| PSTN access code | 9 | Prefix to make an international call in the UK. |
| Operator codes | 0,7800 | Set of numbers to access the local operators. (No blank after comma, or else the subsequent entry is ignored.) |
| Emergency numbers | 999,555 | Set of numbers to access emergency services. (No blank after comma, or else the subsequent entry is ignored.) |
| Initial extension digits | 2,3,4,5,6,8 | 1st digits of numbers that are used for extension numbers on the local node. (No blank after comma, or else the subsequent entry is ignored.) |

### 5.1.2 Canonical Dial Lookup

The following example shows settings suitable for recognizing incoming numbers and assigning them to entries in the local phonebook, and for generating correct dial strings from phone book entries, depending on whether the number is internal or external.

| Parameter | Example value | Explanation |
|---|---|---|
| Local code <1> | 780 | Enterprise node prefix (here: Nottingham). |
| International code <1> | +44115943 | Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN (DID/DDI: direct inward dialing) is 943, which differs from the enterprise node prefix used within the enterprise network. |
| Local code <2> | 7007 | Enterprise node prefix (here: Munich). |
| International code <2> | +49897007 | Equivalent prefix to access numbers on this node from the PSTN. Here, the prefix used by the PSTN for direct inward dialing is identical to the enterprise node prefix. |

#### 5.1.2.1 Conversion examples

In the following examples, numbers entered into the local phonebook by the user are converted according to the settings given above.

**Example 1: Internal number, same node as the local phone**

| | | |
|---|---|---|
| User entry | | 2345 |
| External numbers | | Local public form |
| External access code | | Not required |
| International gateway code | | Use national code |
| Number stored in the phonebook | | +441159432345 |
| Dial string sent when dialing from the phonebook | Internal numbers = Local enterprise form | 1234 |
| | Internal numbers = Always add node | 7802345 |
| | Internal numbers = Use external numbers | 9432345 |

**Example 2: Internal number, different node**

| | | |
|---|---|---|
| User entry | | 70072345 |
| External numbers | | Local public form |
| External access code | | Not required |
| International gateway code | | Use national code |
| Number stored in the phonebook | | +498970072345 |
| Dial string sent when dialing from the phonebook | Internal numbers = Local enterprise form | 2345 |
| | Internal numbers = Always add node | 7802345 |
| | Internal numbers = Use external numbers | 9432345 |

### Example 3: External number, same local national code as the local phone

| | | |
|---|---|---|
| User entry | | 011511234567 |
| External numbers | | Local public form |
| External access code | | Not required |
| International gateway code | | Use national code |
| Number stored in the phonebook | | +4411511234567 |
| Dial string sent when dialing from the phonebook | External numbers = Local public form | 234567 |
| | External numbers = National public form | 011511234567 |
| | External numbers = International form | 004411511234567 |

## 5.2 How to Create Logo Files for OpenStage Phones

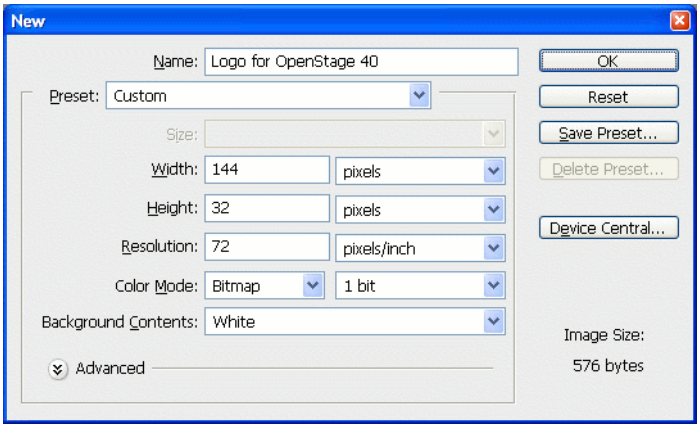
### 5.2.1 For OpenStage 40

**1. Create a New Image**

Create an image with the following specifications:

- Width: 144 px
- Height: 32 px
- Color Mode: 1 bit (monochrome)

**Adobe Photoshop:**




**2. Insert the Logo**

Place the logo image on the background, e.g. by copying it from a source file. Due to the size and color specifications, some adaptations may be necessary.

**Adobe Photoshop Example:**

**3. Save the Image**

Finally, save the image in BMP format. You can now upload the logo file to the phone as described in Section 3.16.7, “Logo”.

## 5.2.2 For OpenStage 60/80

In the following, the creation of a transparent image suitable for use as a logo in OpenStage 60/80 is described. This description is based on Adobe Photoshop, but any similar graphics software can be used as well.

Because of performance issues, half transparency in the alpha channel of the PNG files is not allowed on OpenStage phones. Therefore only 100% transparency or no transparency is used in the phone’s UI elements.

**1. Select the Background Color**

For production purposes, we set the background color to the background color of the skin currently selected on the phone. Later, the background color will be replaced by transparency, which facilitates placing a logo on a gradient background. The following table lists the hexadecimal values, as used in HTML:

| Phone Type | Skin | Color Code |
|---|---|---|
| OpenStage 60 | Crystal Sea | #E7E7E7 |
| OpenStage 60 | Warm Grey | #424242[1] |
| OpenStage 80 | Crystal Sea | #E6EBEF |
| OpenStage 80 | Warm Grey | #3A3D3A |

1 The background color on WP4 - skin 1 is a gradient; the colour listed here is an average value.

**Adobe Photoshop:**

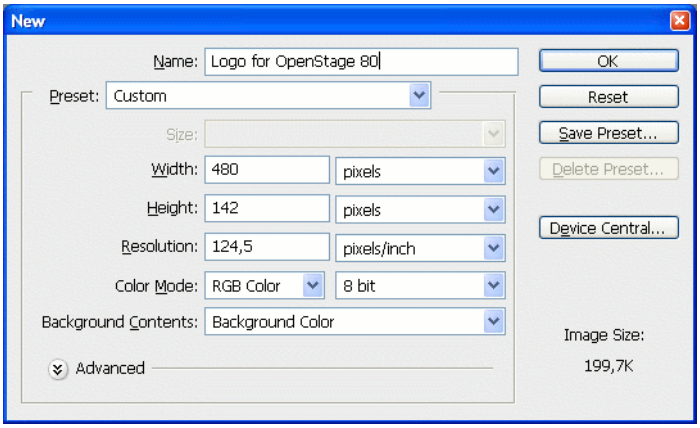
Click on the Background Color icon on the Color palette group, then type the color code without leading "#" into the **#** field)

### 2. Create a New Image

Create an image with the size according to the phone type:

| Phone Type | Size (px) |
|---|---|
| OpenStage 60 | 240 x 70 |
| OpenStage 80 | 480 x 142 |

**Adobe Photoshop:**




### 3. Insert the Logo

Place the logo image on the background, e.g. by copying it from a source file.

**Adobe Photoshop Example:**

### 4. Merge Layers

Merge the two layers to one.

**Adobe Photoshop:**

In the Panel, select both the background layer and the new layer containing the inserted logo. Afterwards, go to **Layer** in the Menu bar, and select **Merge Layers**.

5. **Background Transparency**

   Delete the background colour so that only the exact former background colour is 100% transparent.

   **Adobe Photoshop:**

   Make sure that the background color is selected by clicking on the Background Color icon. In the Tool palette, click on the Eraser symbol with the right Mouse button and select the **Magic Eraser Tool**. After this, got to the Menu bar and set the **Tolerance** field to "0".

6. **Save the Image**

   Finally, save the image in PNG format. You can now upload the logo file to the phone as described in Section 3.16.7, “Logo”.

## 5.3 How to Set Up the Corporate Phonebook (LDAP)

The Corporate Phonebook function is based on an LDAP client that can be connected to the company's LDAP service. A variety of LDAP servers can be used, for instance Microsoft Active Directory, OpenLDAP, or Apache Directory Server.

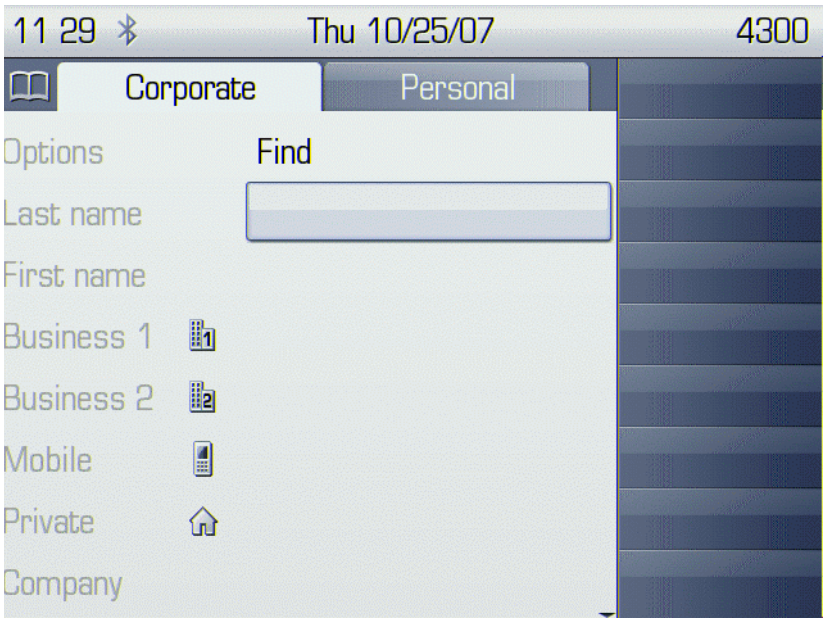
The Corporate Phonebook is available on OpenStage 15/20/40/60/80 phones with firmware version V3R3 onwards.

### 5.3.1 Prerequisites

1. An LDAP server is present and accessible to the phone's network. The standard Server port for LDAP is **389**, the standard transport for LDAP is **TCP**.
2. Query access to the LDAP server must be provided. Unless anonymous access is used, a user name and password must be provided. It might be feasible to use a single login/password for all OpenStage phones.
3. To enable dialing internal numbers from the corporate phonebook, an LDAP entry must be provided that contains the proper number format required by Phone Administration.
   In Microsoft Active Directory, the standard LDAP attribute `telephoneNumber` is typically populated as follows: **+1<area code><call number>**. However, in a standard configuration, Phone Administration will not handle this dial string correctly, due to the **+1** prefix. Therefore, it is recommended to use the **ipPhone** field, which is typically unused in Active Directory. It can be found in the **Telephones** tab of the Active Directory User Manager.

## 5.3.2 Create an LDAP Template

The user interface of the corporate phonebook application provides a form which is used both for search and retrieval.




The task of an LDAP template is to map the phone's search and display fields to LDAP attributes that can be delivered by the server. In the LDAP template, the fields are represented by hard-coded names: `ATTRIB01`, `ATTRIB02`, and so on. These field names are assigned to LDAP attributes, as appropriate.

### Wildcard Quick Search

Supporting a wildcard search for a quick search (V3.3 and upwards) an additional attribute "`ATTRIB12`" is to be set in LDAP template. So it is possible to search for a pattern within a word and not only at the beginning, e.g. 'lea' finds 'project lea der' and 'team lea der'. The addtional attribute "`ATTRIB12`" could be mapped to any attribute of the LDAP server. Therefore the name of any LDAP attribute can be assigned to "`ATTRIB12`" in LDAP template.
The "`ATTRIB12`" is optional, the existing templates remain unchanged, when no wildcard search is desired. Search via FIND-mask is not affected by "`ATTRIB12`". See example → LDAP Template for wildcard search example

The following examples show the relations between GUI field names, the attribute labels used in the template, and exemplary mappings to LDAP attributes.

In an LDAP template for OpenStage 15/20/40, the entries must be sorted according to the sequential number of the template labels, as shown in the example underneath.

### Generic Example (Standard Attributes)

| OpenStage Field | LDAP Template Lables | LDAP Attribute | Example Value |
|---|---|---|---|
| Last name | ATTRIB01 | sn | Doe |
| First name | ATTRIB02 | givenName | John |
| Business 1 | ATTRIB03 | telephoneNumber | 9991234 |
| Business 2 | ATTRIB04 | facsimileTelephoneNumber | 9992345 |
| Mobile | ATTRIB05 | mobile | 017711223344 |
| Private | ATTRIB06 | homePhone | 441274333444 |
| Company | ATTRIB07 | o | Example Inc. |
| Address 1 | ATTRIB08 | departmentNumber | 0815 |
| Address 2 | ATTRIB09 | | |
| Job function | ATTRIB10 | title | Product Manager |
| Email | ATTRIB11 | mail | doe@example.com |
| | ATTRIB12 | any LDAP attribute | **optional** for wildcard search |

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenname"
ATTRIB03="telephoneNumber"
ATTRIB04="facsimileTelephoneNumber"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="o"
ATTRIB08="departmentNumber"
ATTRIB09="l"
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

### Microsoft Active Directory Specific Example

| OpenStage Field | LDAP Template Attribute | LDAP Attribute | Example Value |
|---|---|---|---|
| Last name | ATTRIB01 | sn | Doe |
| First name | ATTRIB02 | givenName | John |
| Business 1 | ATTRIB03 | ipPhone | 9991234 |
| Business 2 | ATTRIB04 | otherTelephone | 9992345 |
| Mobile | ATTRIB05 | mobile | 017711223344 |
| Private | ATTRIB06 | homePhone | 441274333444 |
| Company | ATTRIB07 | company | Example Inc. |
| Address 1 | ATTRIB08 | department | Administration |
| Address 2 | ATTRIB09 | | |
| Job function | ATTRIB10 | title | Product Manager |
| Email | ATTRIB11 | mail | doe@example.com |
| | ATTRIB12 | any LDAP attribute | **optional** for wildcard search |

Given "example.com" as the LDAP subtree to be searched, the LDAP template file looks like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenName"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09="l"
ATTRIB10="title"
ATTRIB11="mail"
EOF
```

### LDAP Template for wildcard search example

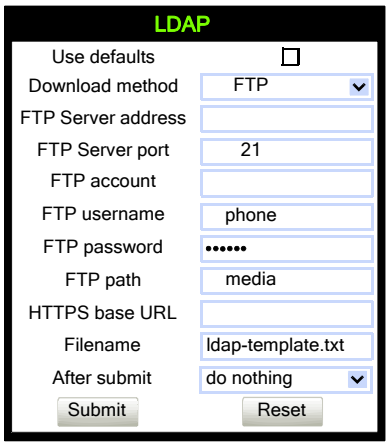
Given "example.com" as the LDAP subtree to be searched with ’wildcard search’ quick search for LDAP attribute ’info’, the LDAP template file looks like this:

```
OpenStage LDAP TEMPLATE (v.1)
SEARCHBASE="dc=example,dc=com"
ATTRIB01="sn"
ATTRIB02="givenName"
ATTRIB03="ipPhone"
ATTRIB04="otherTelephone"
ATTRIB05="mobile"
ATTRIB06="homePhone"
ATTRIB07="company"
ATTRIB08="department"
ATTRIB09="l"
ATTRIB10="title"
ATTRIB11="mail"
ATTRIB12="sn"
EOF
```

### 5.3.3 Load the LDAP Template onto the Phone

When you have configured the LDAP template, you can upload it to the phone:

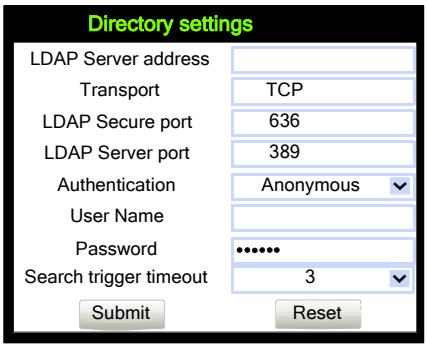
1. Save the template under a suitable name, for example, `ldap-template.txt`.
2. Copy the template file to the FTP server designated for deploying LDAP templates.
3. Upload the file using the WBM (see Section 3.16.6, “LDAP Template”), or, alternatively, the Local menu, or the DLS (see the Deployment Service Administration Manual). For an example configuration, see the following WBM screenshot (path: **File transfer** > LDAP):



### 5.3.4 Configure LDAP Access

To enter the access data using the WBM, take the following steps:

1. Navigate to **Local Functions** > Directory Settings.
2. Enter the following parameters:
   - **LDAP Server address** (IP address or hostname of the LDAP server)
   - **Transport** (allows the LDAP interface to be encrypted using TLS (via LDAPS) or unencrypted using TCP, typically TCP)
   - **LDAP Secure port** (port used by the LDAP for encrypted (TLS) transport, typically 636)
   - **LDAP Server port** (port used by the LDAP for unencrypted (TCP) transport, typically 389)
   - **Authentication** (authentication method for the connection to the LDAP server)
   - **User name** (only required if simple authentication is selected); **Password** (relating to the user name).

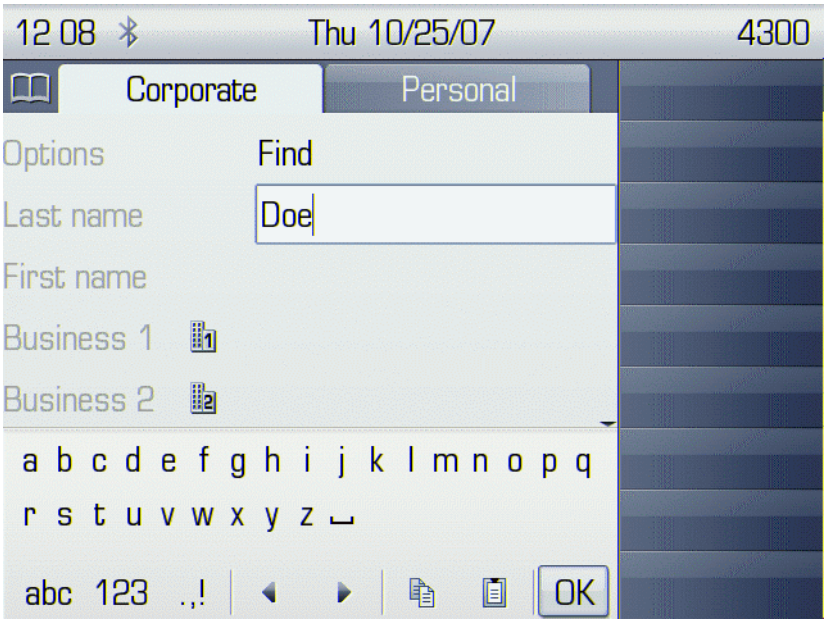



3. Press **Submit**.

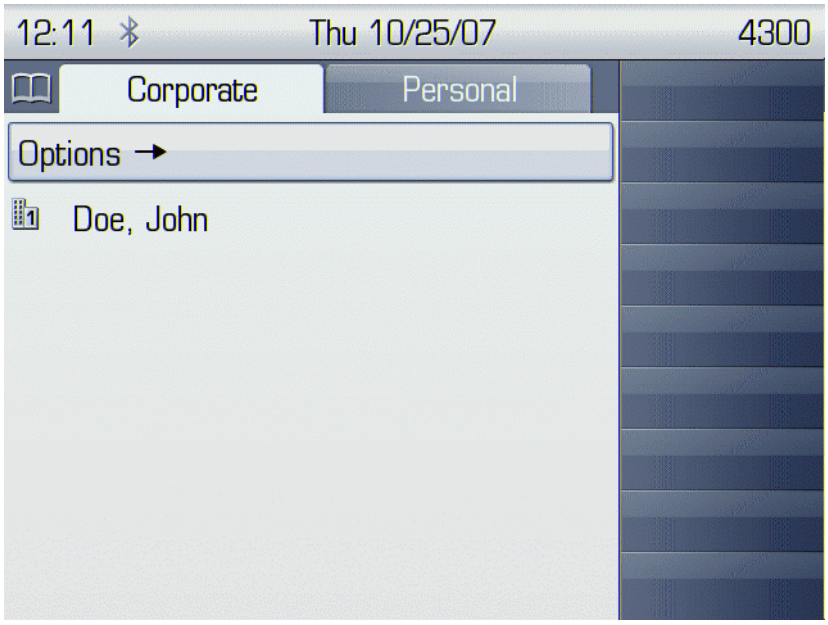
### 5.3.5 Test

If everything went well, you can run a test query on your OpenStage phone.

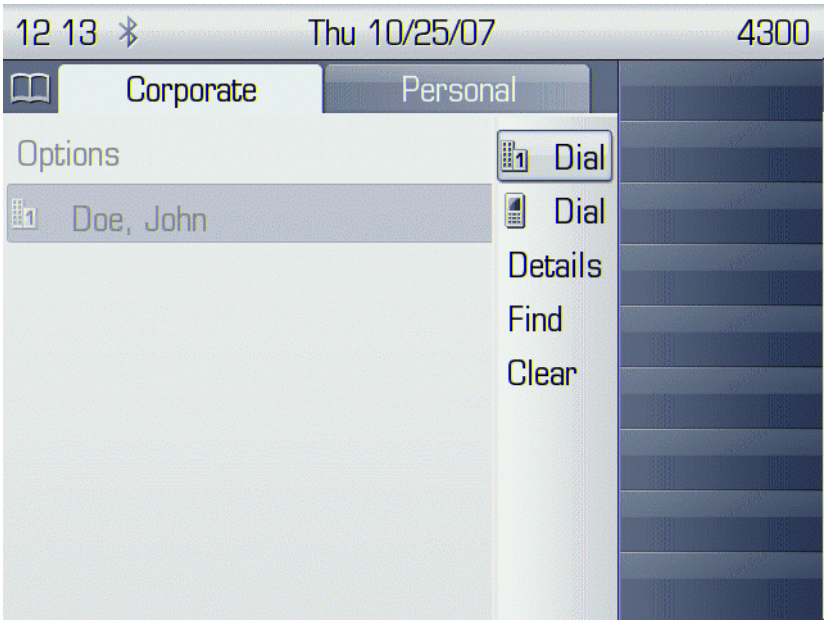
1. To navigate to the phone's corporate phonebook use the following keys: Press the ➔ button until the corporate directory tab is shown (OS60/OS80). Press the "Settings" key or ⊞ on OS15/OS20, or OS40 and use page up/page down to select the corporate phonebook
2. In the query mask, select the entry to be searched, for instance **Last Name**. Press OK to open the onscreen keypad for text input.
3. Enter the text to be searched. For information on using the onscreen keypad, see Section 3.1, “Access via Local Phone”, step 5.




4. Navigate to the Find option and press OK. If the query was successful, at least one entry will be listed in the following manner:



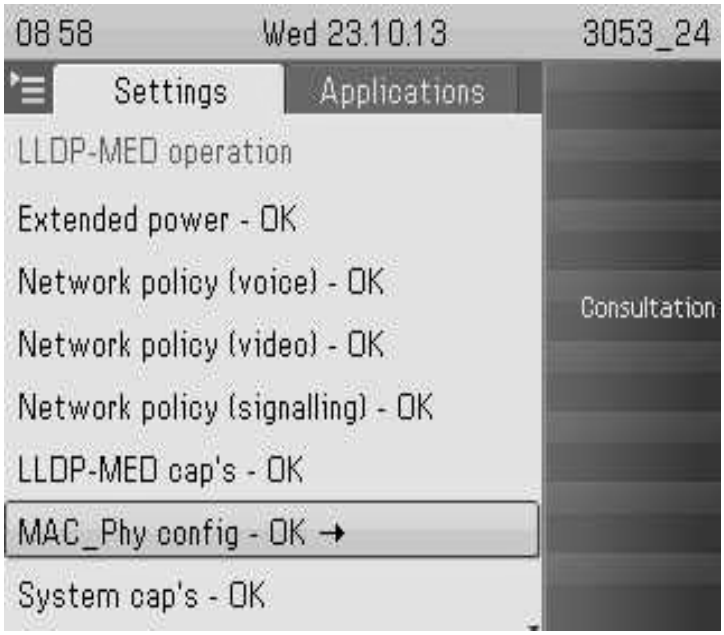
5. Navigate to the desired entry and press ➔ on the TouchGuide to open the context menu. You can select one of the following options:
   - Dial the **Business 1** number.
   - Dial the **Mobile** number.
   - Have the entry's details, that is, all attributes displayed.
   - Start a new search.
   - Clear the list of search results.



## 5.4 An LLDP-Med Example

The following example illustrates the mode of operation of LLDP-MED. In order to evoke a reaction from LLDP-MED, the LAN switch has been set to auto-negotiation, whereas the phone's LAN port (see Section 3.2.1, "LAN Port Settings") is set to 100Mbit/s, hence a fixed value. This configuration error is discovered by LLDP-MED. The following sceenshots from the phone's local menu will show the error messages.

This screenshot shows the LLDP-MED operation submenu (see Section 3.2.3, "LLDP-MED Operation"). Please note the status of **MAC_Phy config**.




When **MAC_Phy config is** selected, the details are displayed.

08 58
Wed 23.10.13
3053_24
Settings
Applications
LLDP-MED operation - MAC_Phy con...
Options
Exit →
AutoSet supported
OK
AutoSet enabled
OK
PMD 0
OK
PMD 1
OK
PMD 2
OK
PMD 3
OK
Consultation

## 5.5 Dial Plan

### 5.5.1 Introduction

A dial plan is a set of rules that determine the phone's behaviour on digit entry by the user. Up to 48 rules are possible. With OpenStage phones, a dial plan rule is constructed from 9 parameters. In the following, the setup of a dial plan is explained.

The dial plan entries are preceded by a title line. This is a free format string, e. g. a descriptive name or version number, which can be used by the administrator for version control purposes.

### 5.5.2 Dial Plan Syntax

The phone will not perform any checking on the title; ensuring that different dial plans are given different titles is part of the administration process.

A dial plan rule is built from the parameters described underneath.

- **Digit string**: A pattern of digits or "*", "#", or "x" characters that is to be matched for starting an action. The maximum length is 24 characters. The "x" character is a wildcard character that represents any of the other digits (it may be upper or lower case).
- **Action** : The action to be taken when the criteria are met. The following options are available:
  - "S" (Send digits): The digits entered are sent to the server when one of the following three conditions is satisfied:

    a) the maximum digits have been received, or

    b) the timer expires after the minimum digits have been received, or

    c) on receipt of the terminator after the minimum digits.
  - "C" (Check for other actions): If the the digit sequence entered by the user matches **Digit string**, **Maximum length**, and **Minimum length**, the timer starts. On timer expiry, the digit string will be sent to the server. If further digits are received before timer expiry, further entries will be checked.
    If the timer is set to 0, the dial string will be sent immediately.
    This option is used when there are more than one rules which start with the same digits.

- **Minimum length**: The dial plan rule will not initiate the sending of digits until at least this number of digits have been entered. However, the digits will be sent after the delay configured in User menu > Configuration > Outgoing calls > Autodial delay (seconds).
- **Maximum length**: Automatic sending will occur when this number of digits have been dialed. If not specified, then the digits will be sent when the timer expires, or a terminating character is entered.

- **Timer**: This indicates the timeout to be used for subsequent digit handling. If not specified, the default timer value is used (User menu > Configuration > Outgoing calls > Autodial delay (seconds)).
- **Terminating character**: A "*" or "#" character which indicates that the preceding digits should be considered complete, even though the maximum length may not be reached. However, the reach the minimum length must be reached by the string built from the digits entered and the terminating characters.
- **Special indication**:
  - "E" (Emergency): If this character is entered here, the digits matching this rule will be sent even if the phone is locked. The number will be dialed immediately even when immediate dialing is disabled, and the phone is on-hook.
  - "b" (bypass): The phone lock is bypassed. The number will be dialed immediately even when immediate dialing is disabled, if the phone is off-hook.
- **Comment**: A remark on this dial plan entry.
- **Terminator sent**: If set to true, the terminating character is sent to the server along with the dial string proper. If set to false, the dial string is sent without the terminating character.

### 5.5.3 How To Set Up And Deploy A Dial Plan

For creating and deploying a dial plan to an OpenStage phone, a working installation of the DLS (version V2R4 onwards) is required. This HowTo describes the creation of a simple dial plan for OpenStage phones by example. Unless otherwise stated, the actions described underneath are made in the DLS.

1. Log on to the DLS with an account that has suitable rights for deploying a dial plan. For details, please refer to the Deployment Service Administration Manual.
2. Navigate to IP Devices > IP Phone Configuration > Features > "Dialplan" tab.
3. Check **Dialplan**, if not checked already.
4. Enter a suitable **Dialplan ID**.
5. Click on to create the first dial plan rule.
6. Enter the following data:

| Parameter | Value | Description/Remarks |
|---|---|---|
| Digit string | 3 | This rule matches numbers beginning with 3. For instance, theses might be internal numbers. |
| Action | S | When all criteria are met, the number is sent to the server. |
| Minimum length | 4 | This rule matches numbers with a length of 4 digits. |
| Maximum length | 4 | |
| Timer | 0 | The specified **Action** will take place without delay when all other criteria are met. |

Summary: This rule determines that digit strings which begin with 3 and have a length of 4 digits are sent to the server without delay after the last digit has been entered.

7. Click on to create the second dial plan rule.
8. Enter the following data:

| Parameter | Value | Description/Remarks |
|---|---|---|
| Digit string | 0 | This rule matches numbers beginning with 0. In the USA, this number calls the operator. |
| Action | C | When **Minimum length**, **Maximum length**, and the length of the digit string entered by the user match, the **Timer** is started. When it expires, the digits are sent to the server. When another digit is entered before expiry, the next dial plan entry will come into operation. |
| Minimum length | 1 | This rule matches numbers with a length of 1 digits. |
| Maximum length | 1 | |
| Timer | 1 | The phone waits 1 second for further digits. If the user does not enter any further digits, the action specified in **Action** is initiated. |

Summary: When 0 is entered as first digit, the phone will wait 1 second. After this, 0 will be sent to the server, which might result in a call to an operator, for instance. When further digits are entered during the 1 second timespan, the next dial plan rule will take control.

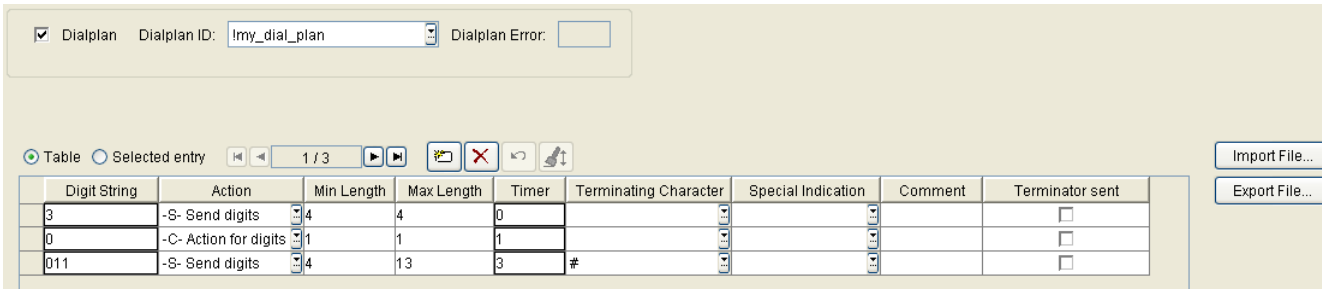
9. Click on to create the third dial plan rule.

10. Enter the following data:

| Parameter | Value | Description/Remarks |
|---|---|---|
| Digit string | `011` | This rule matches numbers beginning with 011. In the USA, this digit string is the prefix international calls. |
| Action | `S` | When the entered digit string reaches the **Minimum length**, the **Timer** is started. On expiry, the digit string is sent. |
| Minimum length | `4` | When the length of the digit sequence entered by the user reaches this value, the **Timer** is started. |
| Maximum length | `13` | When the length of the digit sequence entered by the user reaches this value, the digits are sent to the server immediately. The **Timer** is overridden. |
| Timer | `3` | When the length of the digit sequence entered by the user reaches the **Minimum length**, the phone waits 3 seconds for further digits. If the user does not enter any further digits, the **Action** is triggered. |
| Terminating Character | `#` | When this character is entered, the digits are sent to the server immediately, regardless of the criteria contained in this rule. |

Summary: Any numbers that start with 011 and have a length of 13 digits are sent to the server immediately. Shorter numbers with a length from 4 digits onwards are sent after a 3 seconds delay.

11. The example dial plan is completed; it should look like this:




12. You can check the dial plan using the phone's web interface; navigate to Diagnostics > Fault trace configuration > Download dial plan file.

# Glossary

## A

**Address of Record (AoR)**
A ->SIP ->URI that represents the "public address" of a SIP user resp. a phone or line. The format is similar to an E-mail address: "username@hostname". (for a definition, see RFC 3261)

**ADPCM**
**A**daptive **D**ifferential **P**ulse **C**ode **M**odulation. A compressed encoding method for audio signals which are to be transmitted by a low bandwidth. As opposed to regular ->PCM, a sample is coded as the difference between its predicted value and its real value. As this difference is usually smaller than the real, absolute value itself, a lesser number of bits can be used to encode it.

## C

**CSTA**
**C**omputer **S**upported **T**elecommunications **A**pplications. An abstraction layer for telecommunications applications allowing for the interaction of ->CTI computer applications with telephony devices and networks.

**CTI**
**C**omputer **T**elephony **I**ntegration. This term denotes the interaction of computer applications with telephony devices and networks.

## D

**DFT**
**D**igital **F**eature **T**elephone. A phone with no line keys.

**DHCP**
**D**ynamic **H**ost **C**onfiguration **P**rotocol. Allows for the automatic configuration of network endpoints, like IP Phones and IP Clients.

**DiffServ**
**Diff**erentiated **Serv**ices. Specifies a layer 3 mechanism for classifying and managing network traffic and providing quality of service (->QoS) guarantees on ->IP networks. DiffServ can be used to provide low-latency, guaranteed service for e. g. voice or video communication.

**DLS**

The Deployment Service (DLS) is a OpenScape management application for the administration of workpoints, i. e. IP Phones and IP Clients, in both HiPath- and non-HiPath networks.

**DNS**

**D**omain **N**ame **S**ystem. Performs the translation of network domain names and computer hostnames to ->IP addresses.

**DTMF**

**D**ual **T**one **M**ulti **F**requency. A means of signaling between a phone and e. g. a voicemail facility. The signals can be transmitted either in-band, i. e. within the speech band, or out-band, i. e. in a separate signaling channel.

## E

**EAP**

**E**xtensible **A**uthentication **P**rotocol. An authentication framework that is frequently used in WLAN networks. It is defined in RFC 3748.

## F

**FTP**

**F**ile **T**ransfer **P**rotocol. Used for transferring files in networks, e. g., to update telephone software.

## G

**G.711**

ITU-T standard for audio encoding, used in ISDN and ->VoIP. It requires a 64 kBit/s bandwidth.

**G.722**

ITU-T standard for audio encoding using split band ->ADPCM. The audio bandwidth is 7 kHz at a sampling rate of 16 kHz. There are several transfer rates ranging from 32 to 64 kBit/s, which correspond to different compression degrees. The voice quality is very good.

**G.729**

ITU-T standard for audio encoding with low bandwidth requirements, mostly used in VoIP. The standard bitrate is 8 kBit/s. Music or tones such as ->DTMF or fax tones cannot be transported reliably with this codec.

**Gateway**

Mediation components between two different network types, e. g., ->IP network and ISDN network.

**GUI**
**G**raphical **U**ser **I**nterface.

## H

**HTTP**
**H**yper**t**ext **T**ransfer **P**rotocol. A standard protocol for data transfer in ->IP networks.

## I

**IP**
**I**nternet **P**rotocol. A data-oriented network layer protocol used for transferring data across a packet-switched internetwork. Within this network layer, reliability is not guaranteed.

**IP address**
The unique address of a terminal device in the network. It consists of four number blocks of 0 to 255 each, separated by a point.

## J

**Jitter**
Latency fluctuations in the data transmission resulting in distorted sound.

## L

**LAN**
**L**ocal **A**rea **N**etwork. A computer network covering a local area, like an office, or group of buildings.

**Layer 2**
2nd layer (Data Link Layer) of the 7-layer OSI model for describing data transmission interfaces.

**Layer 3**
3rd layer (Network Layer) of the 7-layer OSI model for describing the data transmission interfaces.

**LCD**
**L**iquid **C**rystal **D**isplay. Display of numbers, text or graphics with the help of liquid crystal technology.

**LDAP**
**L**ightweight **D**irectory **A**ccess **P**rotocol. Simplified protocol for accessing standardized directory systems, e.g., a company telephone directory.

**LED**
**L**ight **E**mitting **D**iode. Cold light illumination in different colours at low power consumption.

**LLDP**
**L**ink **L**ayer **D**iscovery **P**rotocol (IEEE Standard 802.1AB). Provides a solution for the discovery of elements on a data network and how they are connected to each other.

## M

**MAC Address**
**M**edia **A**ccess **C**ontrol address. Unique 48-bit identifier attached to network adapters.

**MDI-X**
**M**edia **D**ependent **I**nterface crossover (**X**). The send and receive pins are inverted. This MDI allows the connection of two endpoints without using a crossover cable. When Auto MDI-X is available, the MDI can switch between regular MDI and MDI-X automatically, depending on the connected device.

**MIB**
**M**anagement **I**nformation **B**ase. A type of database used to manage the devices in a communications network.

**MWI**
**M**essage **W**aiting **I**ndicator. A signal, typically a LED, to notify the user that new mailbox messages have arrived.

## O

**OSC**
**O**pen**S**cape **P**hone

## P

**PBX**
**P**rivate **B**ranch E**x**change. Private telephone system that connects the internal devices to each other and to the ISDN network.

**PCM**
**P**ulse **C**ode **M**odulation. A digital representation of an analog signal, e. g. audio data, which consists of quantized samples taken in regular time intervals.

**PING**
**P**acket **In**ternet **G**ro(u)per. A program to test whether a connection can be made to a defined IP target. Data is sent to the target and returned from there during the test.

**PoE**

**P**ower **o**ver **E**thernet. The IEEE 802.3af standard specifies how to supply power to compliant devices over Ethernet cabling (10/100Base-T).

**Port**

Ports are used in ->IP networks to permit several communication connections simultaneously. Different services often have different port numbers.

**PSTN**

**P**ublic **S**witched **T**elephone **N**etwork. The network of the world's public circuit-switched telephone networks.

## Q

**QoS**

**Q**uality **o**f **S**ervice. The term refers to control mechanisms that can provide different priority to different users or data flows, or guarantee a certain level of performance to a data flow in accordance with requests from the application program. The OpenStage phone allows for the setting of QoS parameters on layer 2 and layer 3 (DiffServ).

**QDC**

**Q**oS **D**ata **C**ollection. A HiPath IP service that is used to collect data from HiPath products in order to analyze their voice and network quality.

**QCU**

**Q**uality of Service Data **C**ollection **U**nit. A service tool that collects QoS report data from IP endpoints.

**QoS**

**Q**uality **o**f **S**ervice. Provides different priority to different users or data flows, or guarantee a certain level of performance to a data flow.

## R

**RAM**

**R**andom **A**ccess **M**emory. Memory with read / write access.

**ROM**

**R**ead **O**nly **M**emory. Memory with read only access.

**RTCP**

**R**ealtime **T**ransport **C**ontrol **P**rotocol. Controls the ->RTP stream and provides information about the status of the transmission, like QoS parameters.

**RTP**

**R**ealtime **T**ransport **P**rotocol. This application layer protocol has been designed for audio and video communication. Typically, the underlying protocol is ->UDP.

## S

**SDP**
**S**ession **D**escription **P**rotocol. Describes and initiates multimedia sessions, like web conferences. The informations provided by SDP can be processed by ->SIP.

**SIP**
**S**ession **I**nitiation **P**rotocol. Signaling protocol for initialising and controlling sessions, used e. g. for ->VoIP calls.

**SNMP**
**S**imple **N**etwork **M**anagement **P**rotocol. Used for monitoring, controlling, and administration of network and network devices.

**SNTP**
**S**imple **N**etwork **T**ime **P**rotocol. Used to synchronize the time of a terminal device with a timeserver.

**Subnet Mask**
To discern the network part from the host part of an ->IP address, a device performs an AND operation on the IP address and the network mask. The network classes A, B, and C each have a subnet mask that demasks the relevant bits: 255.0.0.0 for Class A, 255.255.0.0 for Class B and 255.255.255.0 for Class C. In a Class C network, for instance, 254 IP addresses are available.

**Switch**
Network device that connects multiple network segments and terminal devices. The forwarding of data packets is based on ->MAC Addresses: data targeted to a specific device is directed to the switch port that device is attached to.

## T

**TCP**
**T**ransfer **C**ontrol **P**rotocol. The protocol belongs to the transport layer and establishes a connection between two entities on the application layer. It guarantees reliable and in-order delivery of data from sender to receiver, as opposed to ->UDP.

**TLS**
**T**ransport **L**ayer **S**ecurity. Ensures privacy between communicating applications. Typically, the server is authenticated, but mutual authentication is also possible.

## U

**UDP**
**U**ser **D**atagram **P**rotocol. A minimal message-oriented transport layer protocol used especially in streaming media applications such as ->VoIP. Reliability and order of packet delivery are not guaranteed, as opposed to ->TCP, but ->UDP is faster and more efficient.

**URI**

**U**niform **R**esource **I**dentifier. A compact string of characters used to identify or name a resource.

**URL**

**U**niform **R**esource **L**ocator. A special type of ->URI which provides means of acting upon or obtaining a representation of the resource by describing its primary access mechanism or network location.

## V

**VLAN**

**V**irtual **L**ocal **A**rea **N**etwork. A method of creating several independent logical networks within a physical network. For example, an existing network can be separated into a data and a voice VLAN.

**VoIP**

**V**oice **o**ver **IP**. A term for the protocols and technologies enabling the routing of voice conversations over the internet or through any other ->IP-based network

## W

**WAP**

**W**ireless **A**pplication **P**rotocol. A collection of protocols and technologies aiming at enabling access to internet applications for wireless devices. WAP can also be used by the OpenStage phone.

**WBM**

**W**eb **B**ased **M**anagement. A web interface which enables configuration of the device using a standard web browser.

**WML**

**W**ireless **M**arkup **L**anguage. An XML-based markup language which supports text, graphics, hyperlinks and forms on a ->WAP-browser.

**WSP**

**W**ireless **S**ession **P**rotocol. The protocol is a part of the ->WAP specification. Its task is to establish a session between the terminal device and the WAP gateway.

# Index

## Zahlen

2nd Alert 1-168

## A

Access Control 1-87
Address of Record (AoR) 1-401
Admin Menu (Local Menu) 1-50, 1-51
Admin Password 1-91
Allow in overview 1-172
Alternate 1-155
Application
  Modify 1-254
  Remove 1-255
  Start 1-255
Audio Keys 1-14, 1-15, 1-16, 1-18, 1-19
Audio Settings 1-245
Authenticated Registration 1-109
Automatic VLAN discovery 1-57

## B

Backlight time 1-99
Backup SIP Server 1-121
Blind Transfer 1-156
Bluetooth 1-303
  Advanced Traces 1-292
Bridging enabled 1-179
Bridging priority 1-183
Built-in Forwarding 1-168
Busy Status 1-160

## C

Call
  Accept via Headset 1-158
Call Forwarding 1-152, 1-153
Call Recording 1-148
Call Transfer 1-135
Call Waiting 1-162
Callback 1-137, 1-161
Cancel Callbacks 1-162
Canonical Dial Lookup 1-198
Canonical Dialing 1-194
CCE access 1-87
Certificate Policy 1-94
Character Set 1-92
Cloud deployment 1-45
Cloud service provider, 1-45
Codec Preferences 1-243
Conference
  Phone-Based 1-157
  System based 1-142
Connectivity Check (TLS) 1-117
Connectors 1-22
Consult 1-162
Consultation 1-162
Core dump 1-300
Corporate Phonebook 1-240
CSTA 1-145, 1-401
CTI 1-401

## D

Date and Time (SNTP) 1-28, 1-103
Daylight Saving 1-103
Default Route 1-71
Deflect a Call 1-157
Deployment errors 1-49
DFT (Digital Feature Telephone) 1-401
DHCP 1-28, 1-66, 1-401
Diagnostic 1-261
Dial Plan 1-201, 1-395
Dialing
  Repeat 1-152
  Selected 1-151
Diffserv 1-62
Direct Station Select (DSS) 1-185
Directory Settings 1-240
Display Identity 1-96
Distinctive Ringing 1-204
DLS (Deployment Service) 1-20, 1-78, 1-402
DLS Address 1-29
DNS 1-75, 1-402
  Domain Name 1-75
  Primary/Secundary 1-76
  Servers 1-76
Do Not Disturb (DND) 1-158

Dongle Key (Download) 1-237
Download 1-217
DSS key settings 1-187
DST Zone (Daylight Saving Time Zone) 1-104
DTMF playback 1-245

## E

Easy Trace Profiles 1-278
802.1x 1-290
Bluetooth
Headset 1-279
Bluetooth Handsfree 1-278
Call Connection 1-279
Call Log 1-280
DAS Connection 1-281
DLS Data Errors 1-281
Help Application 1-282
Key Input 1-282
LAN Connectivity 1-283
LDAP Phonebook 1-285
Local Phonebook 1-285
Mobility 1-284
No Tracing for All Services 1-291
Phone administration 1-284
Server based applications 1-286
Sidecar 1-286
Speech 1-288
Tone 1-288
USB Backup/Restore 1-289
Voice Dialling 1-289
Web Based Management 1-290
Emergency Number 1-98, 1-194
Energy Saving 1-99
Error Codes 1-374
External Access Code 1-195
External Numbers 1-195

## F

Factory Reset 1-257
Factory reset 1-87
Factory reset claw 1-87
Fault Trace Configuration 1-271
Feature Access 1-124
Features
Server Based 1-143
Fixed Function Keys 1-170
Forward indication 1-178
Forwarding 1-152, 1-153
FPK program timer 1-150
FTP Settings 1-212
Function Keys 1-14, 1-18, 1-19

## G

G.711 1-243
G.722 1-243
G.729 1-243
Gateway 1-71
General Configuration 1-83
General Information 1-260
General IP configuration 1-69
Graphics Display 1-14, 1-15, 1-16
Group Pickup 1-132

## H

Handset 1-14, 1-15, 1-16, 1-18, 1-19
Hold 1-155
Hostname 1-77
Hot Phone 1-129
Hot warm
action 1-172
destination 1-172
HPT Interface 1-302
HTTP Proxy 1-252
HTTPS Settings 1-212
Hunt Group 1-160

## I

Identity
Display 1-96
Terminal and User 1-96
Immediate Ring 1-185
Initial Digit Timer 1-131
Initial digit timer 1-129
Initial Digits 1-195
Internal Numbers 1-195
International Code (Local Country Code) 1-194
International Gateway Code 1-195
International Prefix (International Access Co-

de) 1-194
IP 1-403
Address 1-27, 1-69
Specific Routing 1-73
IPv4/IPv6 configuration 1-69

J
Join Two Calls 1-156

K
Key Modules 1-192
Keypad 1-14, 1-15, 1-16, 1-18, 1-19
Keys
programmable 1-150
Keyset Operation 1-177

L
LAN 1-403
Monitoring 1-265
Port 1-54
Layer 2 1-61
Layer 3 1-62
LDAP 1-240, 1-384, 1-403
LDAP Template (Download) 1-224
License Information 1-259
Line action mode 1-178
Line Key Configuration 1-171
Line Preview 1-183
LLDP-MED 1-57, 1-60, 1-266
Local Area Code (Local National Code) 1-194
Local Country Code (International Code) 1-194
Local Enterprise Number 1-194
Local National Code (Local Area Code) 1-194
Local Phone Menu 1-360
Logo (Create) 1-380
Logo (Download) 1-227

M
MAC Address 1-404
MDI-X 1-54, 1-404
Media/SDP 1-113
Memory Information 1-269
Messages settings 1-140
MIB 1-404
MIKEY (Multimedia Internet KEYing) 1-84
Missed Call LED 1-307
Mobile User 1-160
Mobility 1-210
Monitoring 1-265
Multiline / Keyset 1-171
Multiline Appearance/Keyset 1-171
Music on Hold (Download) 1-218
Mute 1-169
MWI 1-139
(Message Waiting Indicator) 1-404
MWI LED 1-305

N
National Prefix (Trunk Prefix) 1-194
Navigation keys 1-19, 1-52
Navigator 1-18, 1-51
Network port configuration 1-55
NonCall trans 1-119
Non-INVITE 1-119

O
OCSP 1-94
OCSR failure 1-89
OpenScape Voice (Registration) 1-43
Operator Code 1-194
Originating line preference 1-177
Outbound Proxy 1-111

P
Password
Admin 1-91
Change 1-256
Enter 1-50
Lost 1-257
Policy 1-90
User 1-92
PBX 1-404
PC port 1-54
Phone
Restart 1-257
Software (Download) 1-214
Phone Menu 1-360

Phonebook 1-240
Pickup alert 1-132
Picture Clips (Download) 1-221
PoE (Power over Ethernet) 1-24, 1-405
Port configuration 1-55
Port List 1-372
Power Consumption/Supply 1-24
Preselect
timer 1-178
Preselect mode 1-178
Preview and Preselection 1-184
Preview mode 1-183
Preview timer 1-183
Process
Information 1-269
Program timer (FPK) 1-150
Programmable Keys 1-150
Protocol Mode IPv4/IPv6 1-65
PSTN 1-405
PSTN Aaccess Code 1-194

## Q

QCU 1-81
QoS 1-61
QoS Reports 1-293
Quick Start 1-26

## R

Realm 1-172
Refuse 1-127
Registration 1-43
Authenticated 1-109
Registration Backoff Timer 1-120
Release 1-169
Remote Tracing – Syslog 1-301
Repeat Dialing 1-152
Repertory Dial 1-159
Reservation timer 1-178
Reset Factory 1-257
Resilience 1-116
Response Timer 1-118
Restart Phone 1-257
Ringer
Off 1-155
Ringer File 1-233
RTP 1-405
Base Port 1-242

## S

Screensaver (Download) 1-230
SDES
Configuration 1-86
SDES status 1-86
SDP negotiation 1-86
Secure
file transfer 1-95
SIP server 1-95
Secure calls 1-83, 1-84
Security
log entry 1-89
Security Log 1-88
Selected Dialing 1-151
Send Request 1-165
Server
Authentication Policy 1-95
Server Based Features 1-143
Shared type 1-172
Shift Level 1-157
Shipment 1-22
Show Focus 1-178
Show phone screen 1-169
Silence suppression 1-243
SIP
Addresses 1-106
Ports 1-106
Registration 1-109
Server Address 1-29
Server Addresses 1-106
Server Ports 1-108
Session Timer 1-114
Transport Protocol 1-112
SNMP 1-80, 1-406
SNTP 1-103
SRTP Type 1-84
SRTP type 1-83, 1-84
SSH – Secure Shell Access 1-258
Start Phonebook 1-168
Startup Procedure 1-44
Subnet Mask 1-27

Survivability 1-116

## T

TCP 1-406
Terminal
  Hostname 1-77
  Number 1-27, 1-96
Terminal Identity 1-96
Terminating line preference 1-177
Timeout (Not used) 1-147
Timer
  FPK programming 1-150
Timezone Offset 1-28, 1-103
TLS 1-406
  Connectivity Check 1-117
TouchGuide 1-14, 1-15, 1-16, 1-51
TouchSlider 1-14
Trace Configuration 1-271
Trace Profiles 1-278
Transaction timer 1-119
Transfer on hangup 1-135
Transfer on Ring 1-135
Traps 1-80
Trunk Prefix (National Prefix) 1-194

## U

uaCSTA 1-145
UDP 1-406
Unauthenticated RegistrationRegistration
  Unauthenticated 1-109
Update Service 1-78
Use SRTCP 1-84
User Identifier 1-172
User Identity 1-96
User Password 1-92

## V

Vendor Class (DHCP) 1-30
View Report 1-296
VLAN 1-29, 1-56
VLAN ID configuration 1-59
Voice Mail Number 1-98

## W

Warm Phone 1-129
WBM (Web Based Management) 1-20, 1-26, 1-407
Web Interface Menu 1-311

## X

XML ApplicationsApplications
  XML 1-246
Xpressions 1-246

## Z

Zip Tone 1-164